CYBER OPERATIONS: THE NEW REVISIONIST GRAY ZONE TOOL

A Thesis

Presented to the

Faculty of the College of Graduate Studies and Research

Angelo State University

In Partial Fulfillment of the

Requirements for the Degree

MASTER OF SCIENCE

By

WILLIAM HERBERT LEON LEE

May 2019

Major: Global Security Studies

CYBER OPERATIONS: THE NEW REVISIONIST GRAY ZONE TOOL

by

WILLIAM HERBERT LEON LEE

APPROVED:

Dr. Anthony N. Celso

Dr. William A. Taylor

Dr. Bruce E. Bechtol

Dr. Kishor P. Luitel

25 March 2019

APPROVED:

Dr. Don R. Topliff
Provost, VPAA, and Interim Dean, College of Graduate Studies and Research

ABSTRACT

The weaponization of networked technology is a political tool—still in its infancy—that exists between the realms of hard and soft power. This allows nation-states to achieve strategic objectives without breaking the threshold of an act of war. State sponsored cyber operations are a more aggressive political tool than soft power but not as aggressive as hard power and armed force in most instances. Proper utilization of cyber tools and cyber deterrence can achieve tangible strategic goals that otherwise would only be attainable through physical warfare. This thesis will demonstrate how Russia and China as revisionist powers have successfully utilized cyber in this way, ushering in a new period of nation-state rivalry.

TABLE OF CONTENTS

Page

INTRODUCTION

It is no secret that computers are a defining and ubiquitous aspect of human culture in the 21st century. Nearly all aspects of everyday life involve using a device that contains both a microchip and a networked communication channel to at least one other device, if not the internet as a whole. Most forms of communication between individuals, organizations, and governments are conducted via digital networks—email, Voice over Internet Protocol (VOIP) phones, Military Internet Relay Chat (MIRC), etc. Networked technology is the medium of nearly all communications for government functions from political rallies to tactical combat communications. Beyond communication, an increasingly significant amount of financial transactions, goods, services, education, and information exchange are conducted online.[1] From AirB&B to Facebook, IBM agricultural cloud services to the Supervisory Control and Data Acquisition (SCADA) systems that manage the US power grid and nuclear reactors, the internet is no longer simply a luxury for most modern societies and cultures. It is quickly becoming as fundamental and necessary as roads, plumbing, and electricity.[2]

With technology and invention being a fundamental part of human existence, it has always contributed to inter-state competition throughout history. With the invention of air travel, so began the militarization of aircraft and their use in warfare. When society became dependent on fossil fuels after the industrial revolution, oil became a leveraging tool between

---

1 Schmidt, Eric & Cohen, Jared *The New Digital Age: Transforming Nations, Businesses, and our Lives* (New York, New York: Vintage Books, March 2014).

2 Scott, Laurence *The Four-Dimensional Human: Ways of Being in the Digital World* (London, England: Random House, 2015).

states. In more recent history, nuclear energy and weapons became the focal point of competition and geopolitical deterrence. States have used tools at their disposal along a spectrum of hard and soft power to achieve goals that benefit their respective populations. The internet and the world's reliance on networked technology is no different.

This thesis will argue that cyber operations as an international political tool falls between the realm of soft and hard power and has become the premier tool within a "gray zone" that allows "revisionist powers" to compete without resorting to open warfare.

First, what is a "Revisionist Power" and what is the "Gray Zone?" According to the Institute for the Study of War, revisionist powers "…seek to revise the current global order to their advantage, increasing their regional and global influence while decreasing that of the United States and its allies and partners."[3] The United States has publicly made known that Russia and China are both the premier revisionist powers along with Iran. One of the main methods of seeking the revisionist's goal stated above is through what is called "gray zone" operations.

The Institute for the Study of War defines the "gray zone" as "…the hostile or adversarial interactions among competing actors below the threshold of conventional war and above the threshold of peaceful competition."[4] The gray zone is not a new area of competition nor are cyber operations the only gray zone tool that states use. States who desire

---

3 Dubik, James, Lt Gen, (U.S. Army, Ret.) & Vincent, Nic "America's Global Competitions: The Gray Zone in Context," Institute for the Study of War, (February 2018).

4 Ibid

to change the global status quo without breaking the threshold of war (ie. revisionist powers), use the gray zone to influence their competitors aggressively.

The reason gray zone operations are successful is because they fall under the broader category of coercion. The essence of a gray zone action is commit an action that is small enough for the victim state to decide that the cost of retaliation is not worth it. This allows the antagonizing nation to commit acts that benefit them while not worrying about repercussions. These small acts that fall below the threshold of physical retaliation will then build up until a significant strategic objective is accomplished. By the time the victim state realizes the pattern and what the strategic goals of the antagonizing state are, it is too late to mount an effective response.[5]

An essential part of gray zone operations is ensuring the victim state does not realize the true strategic goals of the attacking state until it is too late. If the victim state realizes the attacker's broader strategic objectives right away, they are more likely to put a stop to it early. Russia heavily uses a deniability concept called reflexive control to further cloud the truth behind their true motives—helping to mask their gray zone objectives. Again looking at the Institute for the Study of War, "Reflexive control causes a stronger adversary to voluntarily choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situation decisively."[6]

---

5 Dubik, James, Lt Gen, (U.S. Army, Ret.) & Vincent, Nic "America's Global Competitions: The Gray Zone in Context," Institute for the Study of War, (February 2018).

6 Snegovaya, Maria "Putin's Information Warfare in Ukraine," Institute for the Study of War, (September 2015).

Russia has a historical reputation for publicly claiming one goal for their actions while an alternative goal goes unnoticed. They attempt to alter the perception of the opposing state in order to influence their decision making. This is a perfect method of operations for successful gray zone actions. Reflexive control historically causes enough ambiguity to slow down or entirely prevent retaliation by other states. When reflexive control is not enough, they resort to full deniability to hide their intentions.

Russia and China both are experts at gray zone operations. Russia has effectively been increasing their sphere of influence in Ukraine, Georgia, Syria, and the Arctic Ocean's Northern Sea Route by committing small acts masked by reflexive control. In most of these cases, the Russians use proxy military groups to further cloud the waters and generally make the situation messier to prevent anyone from attempting to retaliate. While China does not use altered perception tactics as heavily as Russia, they have still utilized the gray zone to slowly start gaining control of the South China Sea (SCS). Similar to Russia's operations in the Arctic, China has started placing military assets in the SCS and has even started building islands to sustain their military presence despite protests from other states. The reason these actions are successful is because each individual action is small enough to either go missed or not warrant the full attention of a state that has the capability to stop them (such as the United States).

How do cyber operations fit within the concept of the gray zone? Just like any toolkit, having a diverse set of options to pick from enables one to achieve a more accurate and precise result. Each tool has certain capabilities and limitations. For certain situations,

specific soft power tools are more suited to achieve a desired goal. Other times, military action or *hard* power may be more appropriate, but a carpenter cannot build a house using solely a hammer and negotiation skills. Other tools become necessary in order to achieve desired results.

Due to the widespread proliferation and dependence of networked technology, "cyber" has become another gray zone tool in the international relations toolkit. What makes networked technology unique, however, is that cyber operations answer a unique question in interstate rivalry that has developed in the post-Cold War era amidst the emergence of revisionist powers. That question is, "When traditional soft power is not enough, how can a nation win objectives against a major state power that possesses military overmatch?"

To answer this question, both Russia and China have found trademark ways to utilize the world's dependance on networked technology and the internet. China primarily has used data theft while Russia has learned to use cyber information warfare operations—sometimes even tied with physical military (or, paramilitary) action.

Due to the relatively cheap cost of cyber operations, smaller nations and even non-state actors have also taken advantage of the cyber warfare tool. North Korea's hack on Sony Entertainment[7] and subsequent threats to US movie theaters for showing an anti-DPRK film resulted in temporary disruption of freedom of speech—several theaters refused to show the film out of fear. Iran has a history of cyber attacks against oil competitors like Saudi Arabia,

---

7 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

and ISIS and other Islamic extremists have effectively utilized social media and mis-information operations to spread ideology and fear. While these smaller cyber threats exist, this thesis will primarily focus on China and Russia through the context of revisionist powers developing cyber tactics for use against the US.

While cyber operations are more aggressive than soft power it has limitations. When used on its own, cyber operations will not—in the foreseeable future—become equivalent to hard power. They will not cause the same level of damage as hard power nor will cyber attacks receive the same level of international response as hard, physical military action. One of the goals of this thesis is to capture both the capabilities and limitations of cyber operations—showing their usefulness as a gray zone tool.

These capabilities and limitations will then be demonstrated and analyzed using historical examples. These examples will be used to capture the tactics, techniques, and procedures (TTPs) that revisionist powers have developed to maximize cyber use's capabilities while minimizing its limitations to achieve strategic goals. These examples will demonstrate that—contrary to public belief and fear—cyber "wars" will not be fought with the same destruction and violence as traditional physical conflict. Cyber operations will play a part in future conflict but, on its own, cyber is best used below the threshold of physical armed conflict.

This analysis will look at cyber operations in three ways. First, how societies use cyber capability will be explored. This section examines how integral networked technology has become to everyday societies. This aspect of the analysis is important because the utility

of state cyber operations is directly proportional its use in society. In other words, a state cannot use cyber operations effectively against a competing nation if the society of that nation does not rely on computers. For example, North Korea has plenty of critical targets within the US to conduct a cyber attack, whereas a US cyber attack on the DPRK would have a more limited effect—North Korea does not rely on the internet to control its electricity or water supply.

The second aspect of cyber use to be analyzed are the technical properties and characteristics of the cyber realm. This includes advantages and limitations of cyber use such as the difficulty of attribution, cost vs effect, the freedom of movement that cyber operations afford, and whether or not cyber operations qualify as "armed force" according to UN articles. This analysis will also break down the stages of a cyber attack and define both terms and the different types of cyber attacks. This will allow for a concise understanding of the fundamental characteristics of the cyber realm in order to understand what it can and cannot achieve.

This will lead to the third aspect of this analysis, the realm of geopolitics. This will be a look at historical examples of how Russia and China have used cyber operations to achieve geopolitical goals and how states might do so more effectively in the future. This third analysis will provide an insight into the two revisionist power's tactics, techniques, and procedures to see how they have leveraged the capabilities of what cyber operations can achieve.

So What?

Why is it necessary to examine state cyber operations as a political tool at all? There are two reasons. First, as this thesis will argue, cyber operations over the past decade have signaled a return of nation-state rivalry that has been out of the spotlight in recent years. After the terrorist acts of 2001 and on, the international focus from the West has been on counterterrorism. However, this same time period of terrorist acts and extremism has also been a period of computer network development behind the scenes. During the international focus on the Global War on Terror (GWOT), states learned to use information war and cyber operations to achieve international effects. Revisionist powers have already begun developing cyber tactics and have begun using this tool in the international sphere. If the international security mindset of the first two decades of the 21st century was focused on counterterrorism, the next decade (or more) will focus on the cyber security threat from foreign states.

The period between 2007 to 2018 saw significant cyber operations committed by several competing state powers. Russia has used cyber operations to cause disruption in Estonia and advanced their projection of military power through cyber attacks in Georgia and Ukraine.[8] During this same period, China has stolen military, industrial, and financial data

8 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

through cyber espionage giving their industries a competitive advantage and employed cyber capability to conduct counterintelligence operations.[9]

This period saw how one state can use cyber and information operations to create fear, confusion, and uncertainty within a rival state. North Korea leveraged stolen data from entertainment company Sony and successfully convinced theaters across the US to obey North Korean demands, temporarily hurting the democratic value of freedom of speech[10] and dictating whether or not theaters would play a certain political film. Russian groups have also manipulated the flow of information across the internet to alter domestic democratic processes in several countries,[11] causing turmoil within the US government and increased mistrust among the US population. ISIS, a non-state actor, successfully used cyber operations to spread their extremist ideology, inciting attacks and fear. Not only did they maximize use of the cyber domain, but they also maximized the use of the media—tailoring their gruesome videos and acts in such a way as to guarantee widespread media coverage.

Possibly the pivotal cyber act of this decade was how the world witnessed the first cyber operation to result in physical destruction of infrastructure—called Stuxnet. This was

---

9 Brown, Ian "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust," War on the Rocks, May 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/.

10 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

11 Jenkins, Tricia "What did the Russian Trolls Want During the 2016 Election: A Closer Look at the Internet Research Agency's Active Measures," War on the Rocks, May 2018, https://warontherocks.com/2018/05/what-did-russian-trolls-want-during-the-2016-election-a-closer-look-at-the-internet-research-agencys-active-measures/.

an attack on a nuclear production facility in Natanz, Iran. The computer virus manipulated programmable logic controllers that managed nuclear centrifuge operation. The malicious code took advantage of several undiscovered exploits to order the centrifuges to operate beyond normal limits—thus destroying themselves. Nearly 1,000 centrifuges were destroyed and Iran's nuclear production at that facility was cut by 20%.[12] Investigators found that the virus had existed as early as 2005 and spent years proliferating thousands of computers around the globe, searching specifically for the hardware used in the Natanz facility before executing. While suspicion for the culprit of the attack has fallen on the US and Israel, neither nation has claimed responsibility for the attack.

Stuxnet was the first cyber attack to cause physical damage to a system. However, it is an outlier within the pattern of cyber attacks and how they've historically been used. Much like the World War II nuclear bombings in Japan, the Stuxnet attacks showed the world the level of damage that cyber attacks could do—and thus nations have been hesitant to use a weapon on that scale since. With the return of nation-state rivalries, the memory of Stuxnet reminds international players of the possibilities associated with cyber attacks.

The second reason why it is necessary to examine state cyber operations is because, as this thesis will argue, geopolitics is the main limiter on what cyber operations will be able to accomplish, not the technical cyber capabilities themselves. In other words, even if nations were to devise ways to bring about severe physical damage to a competing state's

---

12 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

infrastructure while being able to completely conceal evidence or proof, geopolitics and international relations theory will still limit cyber weapons' usage. For example, nations today have the *capability* to invade their neighbors and wage large scale wars to solve geopolitical problems. However, they do not immediately resort to that tactic because geopolitics and international relations drive their decision making.[13] As Kaplan argues, technology does not make geography irrelevant. In fact, technology and the speed at which nations can interact around the world makes knowledge of the geography that drives national strategy all the more important. A return to nation state rivalry means a necessary return to examining what drives a nation's political objectives, because this will shape how that nation uses tools such as cyber operations.

13 Kaplan, Robert *The Revenge of Geography* (New York, New York: Random House, 2013).

PART ONE: SOCIETY'S CURRENT DEPENDENCE ON TECHNOLOGY

The first aspect of cyber operations to be analyzed in this thesis is society's dependence on technology and how this effect cyber utility as a weapon. The more a nation relies on technology for critical needs, the more vulnerable it is to attack though manipulation or disruption of that technology. In a very simplified sense, the cyber realm is somewhat similar to the sea domain of military warfare in this way. A landlocked nation might not reap the benefits of having a deep sea port, but they are also less vulnerable to foreign naval invasion. An island nation may rely extensively on oceanic commerce, but this reliance on the waterways also makes them vulnerable to naval-based foreign actions against them. This does not mean they are helpless against naval attacks. If an island nation appreciates their dependence, they will take defensive measures to make this vulnerability a hard target. However, the mere fact of relying on the sea creates an inherent vulnerability that would not exist otherwise, no matter how strong ones defenses are.

The same goes for networked technology. A nation that fully utilizes technology is inherently more vulnerable to attacks from that domain. Estonia is a perfect example of this. Their heavy cyber dependence for many government functions made them especially vulnerable to Russian attack, which will be examined in this thesis. Much like how a naval-based nation will appreciate their reliance on the sea and take defensive action to shore up their vulnerabilities, a cyber-dependent nation can do the same—creating redundancies in communication lines and backup servers to minimize single points of failure in critical

technologies. However well defended a nation's cyber infrastructure is, though, it is still more vulnerable to cyber based attack than a nation that is not reliant on technology.

As of January 2019, there are estimated to be over 17 billion networked devices around the world. According to the International Telecommunications Union, over 48% of the world population has internet connectivity through some device every month of the year.[14] This includes 41% of the developing world population and 81% of the developed world. Compare this to 2005 when only 16% of the world population was connected, 8% of the developing world, and only 51% of the developed world.[15]

By pure percentage, smaller developed countries have the highest rate of connected device saturation (number of residents having regular internet access compared to population number) with nations like the Falkland Islands, Iceland, and Liechtenstein nearing 100%. Looking beyond these small, developed countries, over 50 nations have a higher than 75% rate of connectivity for their populations as of 2017—with the US taking the number 54 spot at 76% right behind Russia with 76.4%. China in 2017 ranked in the 109th position with a 53% rate of internet connectivity.[16]

This rate of growth is only expected to increase as basic networked technologies become smaller, cheaper, and more proliferated across different industries and markets. Minicomputers, such as the RasperryPi, are only helping speed up the process, allowing users

14 International Telecommunications Union, "ICT Facts and Figures 2017," ITU, 2017, https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

15 Ibid

16 Ibid

with only a basic knowledge of computing to build their own "Internet Of Things" (IoT) connected devices for less than $40 USD. Everything from house lights to vehicles to children's stuffed animals are getting connected to the internet. The immediate threat of proliferated IoT devices such as these may not be immediately evident. The vulnerabilities that the IoT movement poses will be discussed shortly.

What are these populations doing with so many connected devices? After all, quantity of a resource does not necessarily equal vulnerability if the population is not dependent on it. A few main aspects of society where technology has become integral are news and communications, public utilities, and data based decision making.

News and Communications

According to a study conducted by the Pew research center, two-thirds of Americans receive their news from social media. Of that number, 45% specifically listed Facebook among their main news sources. Of that 45%, half stated that they use Facebook as their one and only source of news—not using any other outlet to be informed.[17]

It should be noted that this survey was conducted with a sample size of 4,971 Americans.[18] However, the results of the study are consistent with a larger joint survey and data analysis done by the Swiss National Bank, Reuters, and Columbia University that

---

17 Shearer, Elisa & Gottfried, Jeffrey "News Use Across Social Media Platforms 2017," Pew Research Center, September 2017, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

18 Ibid

included 72,000 participants in 36 countries.[19] This report specifically highlighted Facebook among social media platforms as a predominant source of news information for most people globally. One major limitation of this survey is that they were conducted online, so there is an inherent bias towards people who are already using the internet regularly. However, with the number of connected users nearing 81% of the developed world as seen by the ITU, it is reasonable to say that the survey results are representative of the high majority of the developed world's population.

In addition to news propagation, governments are increasingly relying on internet and social media platforms to communicate and conduct services with their constituents. Taxes and other services are conducted primarily online. Local governments use Twitter and Facebook to quickly disseminate information and receive feedback from the people.

Even outside the government, the internet is the primary medium of communication for the general population. A different Reuters poll demonstrated that 85% of connected users rely on internet communications such as email on a daily basis.[20] 10% of all retail sales in the US were conducted online in 2017.[21] According to Google CEO Eric Schmidt and former Secretary of State Policy Planning Staff member Jared Cohen, the internet will soon become

---

19 Kennedy, Patrick & Prat, Andrea "Where Do People Get Their News?" in 67th Economic Policy Panel Meeting, (Zurich, Switzerland: Swiss National Bank, April 2018).

20 Shearer, Elisa & Gottfried, Jeffrey "News Use Across Social Media Platforms 2017," Pew Research Center, September 2017, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

21 Statista, "E-commerce Share of Total Retail Sales in United States From 2013 to 2021," https://www.statista.com/statistics/379112/e-commerce-share-of-retail-sales-in-us/.

the primary means of commerce, communication, and even employment as more work and service can be done online without a physical presence.[22]

Energy and Utility Control

Moving beyond news and information consumption, the internet is also being used to control and monitor critical services such as energy, water, and other utilities. This is done using supervisory control and data acquisition (SCADA) systems, smart grids, and smart sensors. SCADA systems are software based systems that are used to monitor and regulate infrastructure such as power grids, water supplies, nuclear reactors, etc. These computer programs electronically control physical machinery like pumps, motors, pipeline control flow, and more.

When SCADA systems were first introduced, they were often isolated from the public internet, running on a closed network. This separation made it difficult to install system updates and remotely monitor operations so, more of these SCADA systems are being networked to either an industrial intranet or the even the public internet.

Smart grids, smart sensors, and smart metering are similar to SCADA. According to Symantec, these internet connected components allow utility companies to more accurately and remotely measure energy consumption and provide more minute data to provide robust analysis of flow patterns. This helps give utility companies a better picture of how, when, and

---

22 Schmidt, Eric & Cohen, Jared *The New Digital Age: Transforming Nations, Businesses, and our Lives* (New York, New York: Vintage Books, March 2014).

where energy is being used. Symantec predicts that billions of internet connected sensors and meters will be installed to create smart grids over the next decade.[23]

Agriculture and AI Based Decision Making

Digitally networked sensors and the internet are being used in conjunction with Artificial Intelligence (AI) to collect data and provide granular analysis of large scale systems such as farming. One of the most foundational aspects of every state's economy dating back to the dawn of civilization is agriculture. IBM has marketed their Watson supercomputer and cloud networking services to companies and industries to help inform their decision making with AI powered data analysis.

These complex factors make agriculture a market where advanced data analytics is highly useful. A plethora of factors play a role in decisions such as what crops to grow, where to sow, when to harvest, and more. Everything from global economic changes, population growth, soil conditions, insect behavior, and air quality must be taken into account. Agricultural decisions must also be made with an appreciation for global climate change and its alteration of these aforementioned factors and historical patterns. Using the internet and smart sensors to collect data in conjunction with Watson's advanced ability to analyze such large datasets and their interactions helps farmers to maximize crop yield.[24]

---

23 Wueest, Candid "Targeted Attacks Against the Energy Sector," Symantec, (13 Jan 2014).

24 Mello, Ulisses & Raghavan, Sriram "Bringing the power of Watson to farmers," IBM, September 2018, https://www.ibm.com/blogs/research/2018/09/smarter-farms-agriculture/.

IBM has developed two suites of tools for agriculture industry to use—the Watson Decision Platform for Agriculture and Smart Rural[25]—to provide decision making data based on advanced AI analysis. This data comes both from publicly available information online as well as smart sensors that collect real-time data[26] such as sunlight, condensation, soil quality, pest control, and drone imaging to conduct geographic surveys.

Agriculture is only one market where this advanced, AI-based quantitative information collection, analysis, and decision making is inserting itself into critical industries. IBM continues to advertise their services for markets around the world and, as more and more data becomes available through the proliferation of smart sensors and IoT devices, networked data-based decision making will undoubtedly become the norm for both developed and underdeveloped nations.

The Vulnerabilities of Dependence

The more integral a technology becomes to a society, the more vulnerable they are to attacks through disruption of that technology. In world history, the advent of agriculture made civilizations vulnerable to influences on crop production. When a foreign power wanted to control a people group, they did it though crop yield. After the Industrial Revolution, that control came through oil and fuel as nations looked for ways to power their production, fuel their engines, and make profits selling those resources to other nations.

---

25 Ferkoun, Maamar "Cloud Computing Helps Agriculture Industry Grow," IBM, January 2015, https://www.ibm.com/blogs/cloud-computing/2015/01/23/cloud-computing-helps-agriculture-industry-grow/.

26 Ibid

Now, as societies increasingly rely on the internet for critical industries such as news and communications, public utilities, and decision making for critical markets, networked technology is the new field of control and vulnerability. Internet-based news sources can be manipulated or even blocked out entirely. Communications can be disrupted, causing delays in government functions, financial transactions, or even ability to conduct one's day to day job. Public utilities can be damaged or disabled, leaving populations without power, heat, or working water. Corruption or even theft of sensitive data in critical repositories and decision making engines can result in erroneous decision making or compromise of information that could be damaging to a company or government. These are all within the realm of possibility for a nation that is dependent on networked technology for daily living and critical services.

Even seemingly innocuous IoT devices such as internet controlled vehicles, televisions, and lightbulbs provide a vulnerability. Tests done by McAfee have caused cybersecurity experts to theorize on the possibility of brown-outs if an attacker were to gain access to the wifi-based lighting controls of a population. These experts posited that malicious code could be uploaded onto a computer that is connected to the same local network as the wifi enabled lights. This could be done through an infected email or malicious advertisement. This malicious code would enable remote access to any wifi controlled lights on the network (the code to control these functions remotely already exists). If a threat agent gained access to enough lighting systems on a single section of a power grid, they could—in

theory—cause widespread power outages by activating each device they had access to at one time during peak hours.[27]

Similar techniques could be applied to any smart device. Smart televisions could be remotely manipulated to play a certain propaganda pieces, influential political ads, or maybe interfere with an official announcement such as the State of the Union address. Refrigerators could be powered off remotely to cause widespread food spoilage. When done to a single home or device, the damage is only a nuisance. However, when scaled to a city (malicious code is notoriously easy to spread across a network), mass spoilage of food could cause real concern. Hackers have already demonstrated the ability to remotely control a vehicles speed and braking using the internet.[28] It does not take any imagination to see the damage such an attack like that would cause.

The above are all simply examples of what is within the realm of the possible when a nation is dependent on networked technology for critical services and infrastructure. Part three of this thesis will look in more detail at how cyber operations and the above vulnerabilities have actually been exploited by revisionist powers in the past decade.

---

27 Siskind, Geoff "Hackable Podcast by McAfee," McAfee, February 2019, https://hackablepodcast.com/.

28 Greenberg, Andy "Hackers Remotely Kill a Jeep on the Highway—With Me In It," Wired, July 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

PART TWO: CYBER TERMS, DEFINITIONS, AND TYPES OF ATTACKS

Before continuing on with an analysis of the unique characteristics of the cyber realm and how revisionist powers have used it, it is necessary to establish some basic terms and definitions. This section will define cyber warfare, cyber attack, break down the actual steps and methodology of a cyber attack, and define some of the more common types of cyber attacks that will be discussed throughout the rest of this thesis.

The definition of cyber warfare that this thesis will operate on is provided by Richard Stiennon in the book, *Cyber Warfare: A Multidisciplinary Analysis,* "Cyber warfare is an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direct or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)."[29]

Furthermore, a cyber attack is defined as:

> "An electronic attack to a system, enterprise or individual that intends to disrupt, steal or corrupt assets where those assets might be digital (such as data or information or a user account), digital services (such as communications) or a physical asset with a cyber component (such as the process control system found in a building, aircraft or nuclear refinement facility). Typically such attacks seek to compromise the

---

29 Stiennon, RIchard "A Short History of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

confidentiality, integrity or availability of digital assets, and so cyber security controls seek to preserve these properties in some way."[30]

Finally, the term "electronic" within the above definition refers to the use of energy to transmit information. This includes electronic data (computer code) that is sent across networks to conduct the attack.[31]

Stages of a Cyber Attack

There are typically four stages to a cyber attack: reconnaissance, exploit delivery, payload injection, and iteration.[32] Reconnaissance is a necessary part of part of cyber attacks in much the same way as it is in soft and hard power actions. Whereas a military targeteer uses known information on a facility to determine the type of munition used in bombing that target (construction material of the building, whether it is hardened, surrounding area, etc), the type of cyber attack used is typically suited to the specific hardware and software being used by the target. In other words, not every type of attack works against every type of network or computer. Additionally, the method of delivery must be analyzed (for example, can the malicious code be delivered via the internet or is there an "air gap" requiring the payload to be physically uploaded onto the local system or network) as well as other factors.

---

30 Stiennon, RIchard "A Short History of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

31 Ibid

32 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

In the case of social engineering (to be further defined in the next section) and misinformation operations, reconnaissance must also be done on the targeted individuals. Social engineering attacks such as spear-phishing (where the target receives an email containing false information designed to entice the target to disclose sensitive information such as bank numbers or passwords) have a higher chance of success when there is sufficient knowledge on the target to craft a convincing email.

An attacker must be careful when conducting reconnaissance not to raise too many flags that might tip off the defender to an impending cyber attack. A balance point must be made between gaining sufficient intelligence on the target and giving away one's intentions. Additionally, if reconnaissance actions can be traced back to the attacker, then attribution is easier to determine when the attack is actually made.[33]

The second stage of a cyber attack is exploit delivery. This is where the actual cyber defenses of the target are compromised—creating a path or opening for the attacker to gain access the victim system or network. The tool or vulnerability that the attacker uses to gain access to a system is called the exploit. Exploits come in various forms from inexpensive, commercial off the shelf software tools to highly valuable "zero day" exploits—vulnerabilities in a computer system that have yet to be patched or even discovered by the manufacturer or user.[34]

---

33 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

34 Ibid

Separate from the exploit delivery is the payload injection. While the exploit is the method of compromising the target's cyber defenses and gaining access to their system, payload injection is the insertion of malicious script such as a program designed to corrupt data, spyware tools like keyloggers, or other types of viruses.[35]

Within the payload injection stage, some attacks may also be designed to have persistence while others may be designed to destroy themselves to prevent discovery. Persistence allows future access to the compromised system without having to repeat the exploit delivery stage of bypassing the target's security. A payload can be designed to reside on the system and avoid detection and deletion in order to allow for indefinite access to the target system for attacker manipulation.[36]

The final stage of a cyber attack is iteration. This is what the malicious code does after it has been executed. A virus may be designed to allow remote access of the targeted system for an indefinite period. Some payloads may be designed with persistence to conduct further reconnaissance and map out the network it has infiltrated. Some other payloads may be designed to establish new avenues of exploitation to allow for easier future access. Still other payloads may be designed to reconfigure themselves in order to further exploit other

---

35 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

36 Ibid

portions of the network in which it resides in order to deliver a second payload in another portion of the infected system.[37]

These four stages of a cyber attack: reconnaissance, exploit delivery, payload injection, and iteration, have been broken down in and incorporated into other attack models by different security firms such as Lockheed Martin's seven-step "Cyber Kill Chain."[38] However, the above four stage process has been chosen in this thesis for its simplicity in order to provide a surface level understanding of cyber attack methodology.

Often the most difficult part of a cyber attack is the exploit delivery phase that grants access to the targeted system. Most tools and resources that hackers incorporate are used to gain initial access into a system. To conduct a successful exploit, there are six questions that a perpetrator must consider in deciding what type of tool he wants to use.[39] The reconnaissance stage of a cyber attack helps the perpetrator to determine the answers to these questions:

1. How targetable is the exploit? This is the ability of the attacker to target only the intended exploit. Similar to the idea of "collateral damage" in hard power and "unintended

---

37 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

38 Hutchins, Eric "The Cyber Kill Chain," Lockheed Martin, 2019, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

39 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

consequences" in soft power, the ability to be as precise as possible in a cyber attack helps to ensure maximum efficiency and also keeps the fingerprint of the attack as light as possible to maximize covertness—if that is a desired attribute of the cyber attack.[40]

2. How much control does the attacker have over the exploit? The controllability of an attack that is executed further enables the perpetrator to be precise in which systems are manipulated or which data gets wiped or stolen. If an attacker wants to steal a specific computer file at a firm but the only tool in his disposal is a malicious program that, once executed, steals all the data available on the compromised network, then the attacker has low controllability over the exploit and his chances of discovery are increased. Certain attacks may not require a significant amount of controllability depending on the goal of the attack.[41]

3. How persistent is the exploit? There are two aspects to persistence. Persistence of the exploit and persistence of the payload. Persistence of the exploit refers to how long the targeted system can remain compromised before the defender is able to fix their cyber defenses. Persistence of the payload refers to how long the payload can remain on the system undetected and, if detected, how difficult it is to remove. If the defender simply needs to change his password in order to eliminate the attacker's ability to access the target system, then the attack has low exploit persistence. If the payload is easily discovered and

---

40 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

41 Ibid

can be removed completely by rudimentary anti-virus software, then the attack has low payload persistence.[42]

4. What is the effect of the exploit? Again, it is important to distinguish the difference between the exploitation and payload here. The effect of the exploit is the consequences of compromising the target system. The effect of the payload is the desired manipulation of data after access to the system has been achieved.[43] The effect of the exploit is important to factor in because, if the attack requires a high level of covertness in order to accomplish its geopolitical goal but the exploitation of the network that is necessary for the attack to happen will be highly visible, then the attack and its goals will not align and it will fail to serve its geopolitical purpose. Sometimes, the attack is not worth the effort it takes to exploit the network.

5. How covert is the attack? Covertness may be a desired attribute depending on the geopolitical goals of the attack.[44] Other times, lack of attribution may be more important than hiding the fact that the attack took place at all. However, in this context, the question refers to concealing the fact that the attack is in progress. It is desirable in nearly all instances that the target not be aware that their systems are being compromised until after

---

42 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

43 Ibid

44 Ibid

the attack has taken place. Determining the level of covertness desired in execution of the attack is directly related to how aggressive the attacker wants to be in his reconnaissance.

6. How mitigable is the exploit? This question determines how capable the target is in preventing exploitation. How strong or redundant is the cyber defense that the attacker is planning on overcoming or bypassing? A simple example is having a strong password. If the attacker is planning on exploiting a system by determining the target's password, the attack can be easily mitigated by the target using a strong of a password as possible and having software that prevents "brute force" attacks that try as many password combinations as possible.[45]

Types of Cyber Attacks

Now that the methodology of a cyber attack has been established, it is helpful to define broadly the different types of common cyber attacks that will be discussed in this analysis. The main types of attacks and terms to be discussed in this paper are malware, Distributed Denial of Service attacks, social engineering attacks (phishing, spear phishing, whaling, etc), and System Control and Data Acquisition (SCADA) attacks.

Malware

In the public discourse, malware and viruses are often used interchangeably. However, malware is actually a general term for any type of malicious software that the

---

45 Hodges, Duncan & Screese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis* (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

owner of a device did not authorize the installation or use of. A computer virus is a specific type of malware. A virus is the term used to describe malware that spreads from the host system to other computers. Further specific types of malware include trojans (malware designed to appear safe so the user and the computer's security system do not notice the threat), ransomware (malware that restricts access to the user's data), and spyware (malware that monitors the user's activity such as keystroke loggers). Hitherto in this paper, the term malware will be used for describing, in general, unauthorized malicious code or software.

DDOS

Unlike malware, a Distributed Denial of Service attack, or DDOS, does not always involve injecting malicious code onto the target computer or network. One of the most common types of cyber attacks, a DDOS happens when too many hosts try to access a server all at once, causing a system or website to crash. While a DDOS can happen if enough real world users try to access a site at one time, this type of attack usually occurs though one attacker having access to hundreds or thousands of compromised computers—often called botnets—and instructing them all to access the targeted server.

Starting with one computer, the attacker loads light-footprint DDOS tools onto vulnerable systems through the internet often unnoticed by the infected system's owner. Each compromised system becomes part of the botnet and contributes to the overloading of the target server. Because of the relative simplicity and low cost of DDOS attacks, they are commonly used by lone actors as well as states. Often, they are conducted to disrupt a company (often a financial institution) or state's online service.

Social Engineering Attacks

Social engineering attacks are designed to trick users into giving away private information or unwittingly downloading malware. These attacks most often occur through emails. For example, the attacker will design an email falsely claiming to be from the user's bank. The email will state that there is an issue with their account and that they need to call a specific number or click on a link to a website where the user inputs their banking information thinking that they are communicating with their bank. The attacker may also send attachments disguised to look both harmless and something of interest to the user, such as an invoice for a recent purchase. When the user downloads the attachment, malware is installed onto their system.

Social engineering attacks can vary from generic emails sent to many people (phishing), specifically tailored communications designed to look legitimate to one specific person (spear-phishing), or even target high-value/high-profile individuals such as CEOs or political party members (whaling).

SCADA

SCADA attacks are possibly the most difficult and complex type of cyber attack to date. For their complexity, they can also have the highest payoff—resulting in physical damage to infrastructure as opposed to other cyber attacks whose damage is limited to espionage or data and communication disruption.

If an attacker gains access to a SCADA system, they can manipulate machinery to operate outside of normal parameters to fail, or simply shut them down. Depending on the system that is compromised, this can result in power outages, lack of clean water, commuter train derailment, and more.[46]

As the global cyber threat becomes more realized, digitally networked critical infrastructure is increasingly being secured, making SCADA attacks more difficult for all but the most well-funded state sponsored hackers. The capabilities of conducting such attacks are lucrative to states for the widespread infrastructure disruption they can cause.

Unique Characteristics of the Cyber Realm

What characteristics of the cyber realm make it a useful tool for state use? Beyond society's reliance on technology for the execution of critical tasks, what are some of the unique factors to consider when a state executes, or falls victim to, a cyber attack?

First, cyber operations are relatively cheap. This is true both in monetary value and oftentimes in terms of manpower and risk versus reward. All it requires is the right hardware (which increasingly drops in price every year) and technically capable operators. Compared to other state tools, such as military power, cyber operations have an incredibly low barrier of entry to where nearly every state can quickly and cheaply establish a viable cyber operations program.

---

46 Yardley, Tim "SCADA: Issues, Vulnerabilities, and Future Directions," Login Vol 33, no 6. (December 2008).

Second, because cyber operations typically travel via global networks, they often allow for a wide degree of virtual freedom of movement. This virtual freedom of movement not only allows two geographically divided areas to interact in ways they couldn't otherwise but also allows for operation within a third country—sometimes without their knowledge.

This leads to the third benefit, manipulation or masking of attribution. While the majority of cyber attacks have historically left trace clues that amount to circumstantial evidence, the accused state can often blame proxies that have little to no "official" tie to the state. Even worse, the attacking state can leave false evidence implicating another state.

Lastly, cyber operations provide for a new avenue of subversion and information warfare that offers unprecedented penetration of the target audience to be manipulated. One well-designed piece of foreign propaganda can find itself in the pockets of hundreds of millions of citizens within a span of minutes from creation to dissemination. Social media tools are specifically designed to maximize the exponential spread of ideas. For this reason, there could not be a more perfect delivery tool for anyone wanting to spread subversive mis-information.

Unique Characteristics of the Cyber Realm: Cost, Risk, and Effect

Cyber attacks range from a spectrum of fairly simple DDOS attacks to incredibly well-planned out and sophisticated SCADA attacks such as Stuxnet. In general terms, the simpler a cyber attack, the less expensive it is. The costs of state funded research and development of hacking tools varies depending on the target and is difficult to asses.

However, observations of the black market allow some level of insight into the general cost. According to Kapersky Labs, a DDOS attack can be purchased on the black market for $25 an hour.[47] The cost of creating a DDOS attack on one's own is estimated to cost as little as $7 an hour. This price varies depending on the number of computers one wants involved, the severity of the attack, and other factors. On the other end of the spectrum, a RAND study found that zero-day exploits can cost up to several thousands of dollars.[48]

The cost of cyber hardware is also cheap in relative terms compared to military weapons and equipment. As seen earlier in this paper, the cost of technology is continually dropping to the point that even developing nations can afford networked computing. Many cyber attacks do not require state of the art hardware. In fact, many hacking tools can be run on a Linux-based Operating System called "Kali." Linux operating systems are well known for their ability to run on outdated, cheaper computer hardware and are a popular choice for users of aging machines that do not have the power to run newer Windows and Macintosh operating systems. In fact, a lightweight version of the Kali OS can even be installed on the aforementioned Raspberry Pi minicomputer which costs less than $40 USD.

As far as risk goes, the less sophisticated, cheaper attacks typically do not cause permanent damage and historically leave no lasting effect. DDOS attacks, for example, only temporarily disrupt websites and communications. These low complexity attacks also have

---

47 Barysevich, Andrei "Dissecting the Costs of Cybercriminal Operations," Recorded Future, November 2017, https://go.recordedfuture.com/hubfs/cyber-operations-cost-appendix.pdf.

48 Blue, Violet, "Hackonomics: Street Prices for Black Market Bugs," ZDNet, April 2014, https://www.zdnet.com/article/hackonomics-street-prices-for-black-market-bugs/.

the benefit of better attribution hiding. DDOS attacks utilize hundreds, sometimes thousands of computers that are often spread across the globe so finding the source of the attack sometimes can be complicated and evidence is typically circumstantial at best. Attack tools for DDOSes are also so widely proliferated that it is difficult to identify the source based on the design of the attack—like one could possibly do with complex, uniquely tailored attacks that could have only been accomplished by a small list of actors. This attribution is also made more difficult when a state utilizes "independent" parties to conduct the attacks. Both China and Russia have groups that have no official ties the government yet still are suspected of carrying out attacks on their behalf.[49]

Because of the difficulty of attribution and the fact that there is no permanent physical damage done, most cyber attacks carry very low risk for the attacker. No nation has responded with physical violent escalation in retaliation to a DDOS attack.[50] Historically, if these attacks are retaliated against at all, it is only with more DDOS attacks. For instances of data theft, retaliation is usually done though federal indictments or, at most, limited effect sanctions.[51] This makes most cyber attacks incredibly lucrative. A nation state can disrupt networked communications, conduct surveillance and even steal data for little monetary cost

---

49 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

50 Ibid

51 Bartz, Diane & Stubbs, Jack, "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies-idUSKCN1OJ1VN.

and without fear of any significant international backlash. For revisionist powers, the risk is well worth the reward.

If used in conjunction with other types of action, such as when Russia used DDOS attacks in concert with military actions in Georgia,[52] the benefits of these attacks are heightened because the attacker is now disrupting target communications to increase the fog of war and weaken the enemy in supplement to military forces. However, this can come at the cost of attribution because it is then easy to connect the cyber attack with the military attack—though Russia still used third parties to conduct these attacks to maintain some level of deniability.[53]

On the higher end of the cost-risk-reward spectrum are sophisticated types of cyber attacks that are designed to do significant damage against a highly hardened and secure target. In order to be successfully executed, these types of attacks typically need to be specially tailored to their specific target down to the make and model of routers and switches and require extensive research and design to counter the target system's defenses. Stuxnet—which stands as a cyber attack outlier due to its extreme complexity and physical effects—is the most popular example.

Attacks on this level of complexity carry much higher cost and risk than the attacks discussed thus far in this section. First, attribution is easier. The more complex and advanced

---

52 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

53 Ibid

the attack is, the shorter the list of potential suspects with the capabilities and manpower to undertake such attacks. While anyone can conduct low to mid level cyber attacks, it takes considerable resources to design an attack on the scale of something like Stuxnet. An additional factor increasing attribution is that these attacks typically need to be specifically designed against the target. As will be discussed in the next section on attribution, the designers of one of a kind tailored attacks will typically leave behind digital fingerprints that give away the country of origin.[54] This is an additional risk that more proliferated cyber attacks do not carry.

Another issue increasing the cost of the more highly complex cyber attacks is their limited use and shelf life. Unlike conventional weapons, many complex cyber tools cannot sit in a warehouse and wait to be used. Due to constant changes in technology, cyber tools will quickly become obsolete if the software they are designed to work against gets updated. The Stuxnet attack utilized several zero day exploits. The problem with "zero days" is that, once they are used against a target or otherwise discovered, the victim will patch the vulnerability to prevent a second attack. For this reason, many zero day exploits can only be used one time —unlike conventional weapons or even less complex cyber attacks that use inherent vulnerabilities that cannot be eliminated. An additional complication of zero days is that, the longer the exploit goes unused, the greater the risk that the target realizes the vulnerability on their own and fixes it themselves, rendering the zero day useless. For this reason, once an

---

54 Rowe, Neil "The Attribution of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

attacker has invested the time and effort to develop a cyber attack that utilizes zero day exploits, they have incentive to use the attack sooner rather than later.[55] Thus, complex attacks that use zero days carry more cost and risk.

With the exception of these highly complex attacks, the vast majority of cyber operations can be carried out with significantly less cost and risk than other forms of International action such as conventional military operations and complex economic policies while reaping significant rewards. For relatively few dollars and very little risk of retaliation, a state can steal sensitive personal, corporate, and government information, spread propaganda, influence democratic processes, and disrupt vital communications. With this in mind, it seems an easy choice for a revisionist state to begin conducting cyber operations.

Unique Characteristics of the Cyber Realm: Attribution

Perhaps the most widely discussed advantage of cyber operations is the appearance of anonymity, plausible deniability, and misattribution of cyber attacks. There are multiple reasons this is possible. First, cyber networks are connected across international borders and contain within them civilian, industrial, and military information data all along the same digital connections. Second, many low level "off the shelf" cyber attacks are widely proliferated among the civilian black market. This means that, when a state uses these attacks, it is more difficult to analyze the computer code to find clues indicating the origin of the attack. Even worse, a state can manipulate the digital fingerprints to implicate a different

---

55 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

nation in what is called a "false flag" operation. Third, unlike physical weapons and conventional military resources and tactics, computer programming skills exist across the civilian and criminal world in addition to governments. Some states have taken advantage of this, using proxy organizations with no official ties to the government to conduct cyber operations allowing for the state to have deniability. If an attack gets traced to its source, the state can simply claim that it was conducted by rogue criminals who were not acting on behalf of the state, even if the result of the attack benefits that state.

Attribution: Global Connectivity

The first obstacle in gaining attribution to cyber attacks is the fact that these attacks are sent and occur across a global network. If "nation A" was to conduct an attack against "nation B" on the other side of the globe, the malicious code may travel through multitude of other nations, internet service providers, and even reside long-term on other physical computers before the attack reaches its intended target. The Stuxnet virus is estimated to have taken months from its initial release to it infecting the nuclear site at Natanz[56] and it infected over 200,000 computers in over 8 countries along the way.[57]

Because of this global connectivity, it is easy for an attacker to forward position himself in virtual space to begin an attack from within another country's cyber network. If an attacker gains access to a computer located in another country, he can then use that victim

---

56 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

57 Ibid

computer to begin launching the malicious code—further masking the source. Even if an attack is accurately traced to the correct terminal of origin, there is no guarantee of who was sitting behind that computer, developing and executing the attack. Someone acting on behalf of the Russian government can utilize a computer with a German-based Internet Protocol (IP) and MAC (Media Access Control) address to conduct an attack on Ukraine.

Attribution: Digital Fingerprints

Digital fingerprints that can be analyzed following an attack can help find attribution for an attack, but it can also lead to false clues and mis-attribution. The past decade has seen a variety of cyber attacks that range in sophistication. As a general rule, less sophisticated attacks utilize open-source, proliferated scripts that require little tailoring to the target to be effective. On the other end of the spectrum are complex attacks against hardened targets that require significant planning, research, and original coding.[58] Because the sophisticated attacks require such planning, customization, and original work, it is often possible to analyze the script of the attack in order to determine the originator. According to Kapersky Labs, "A combination of certain features of the code development environment stored in the files can be used as a 'fingerprint,' in some cases identifying the malware authors and their projects".[59] For example, several attacks have been attributed to Russia due to the fact that

---

58 Rowe, Neil "The Attribution of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

59 Bettencourt, Jessica "The Olympic False Flag: Infamous OlympicDestroyer Malware Designed to Confuse Cybersecurity, Community," Kapersky Labs, March 2018, https://usa.kaspersky.com/about/press-releases/2018_the-olympic-false-flag.

there were Russian terms and language in the code. In another instance, metadata for certain malicious programs indicated that most of the code was written in what would have been daytime working hours in the Moscow time zone and never on Russian federal holidays. This indicates that the source might have been Russian state sponsored actors whose day to day job is to attempt to hack into foreign systems.[60]

Therefore, the more advanced the attack, the more evidence there is to discover some level of attribution in general. Additionally, when an attack is complex, it limits the list of who the possible perpetrators are. Like with military resources, while many nations have some form of cyber capability, they have varying levels of cyber prowess. For this reason, an attack as complicated as Stuxnet could only be attributed to a small group of nations and organizations and was far too complex to be executed by certain other players. Once an investigator factors in the target of the attack and suspected geopolitical goals, that list is further narrowed down to only one or two possible nations.

Even when the attack is traced to a third party (such as a criminal group or civilian hacker organization) with no official association to a state government, the suspected goal of the attack, geopolitical analysis, and historical precedence provides enough circumstantial evidence for the target nation to publicly accuse a suspected state of collaborating with that third party. Most of the "independent" groups responsible for carrying out cyber attacks that have benefited a state have been found to posses hidden ties with national governments. Even

---

60 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

if no direct tie can be established between a proxy group and a state, the suspected offending state can still be accused by the victim state of not preventing criminals from carrying out cyber attacks within their territory. Either way, the victim state typically has circumstantial evidence to carry out some form of political action against the offending state. Usually, this retaliation is done through federal indictments.[61] These political retaliations have thus far, done little to stop or slow a nation down from conducting attacks.

Overall, while lack of attribution has been touted as a high advantage of cyber operations, history shows that most major attacks have been at least circumstantially attributed enough for the victim state to take political action against the suspected perpetrator. That being said, one additional factor should be discussed when it comes to the advantage of attribution—false flag operations. There has been much speculation on the possibility of a state carrying out a cyber attack and leaving false clues for the victim state to follow and attribute cause to a third, uninvolved state. In theory, the real perpetrator may want to do this in order to provoke two states into a conflict that would benefit the true originator of the attack. This is theoretically possible because most evidence that has been discovered when analyzing cyber attacks thus far has been circumstantial at best. By analyzing what evidence has been used in attributing past attacks, a state can plant false clues in the attack. For example, attacks on Ukraine and the US elections have been attributed to Russia because of

---

61 Bartz, Diane & Stubbs, Jack, "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies-idUSKCN1OJ1VN.

Russian terms in the coding and the code being scripted during Moscow daytime hours.[62] Knowing this, a future state that wants to provoke strife between two states can make sure to include linguistic terms in the code and design and execute the code during the time zone that fits whatever nation the perpetrator wants to implicate.

Attribution: False Flags

There is evidence of groups (possibly states) attempting false flag operations with limited success. One example was found by Kapersky Labs in analyzing the OlympicDestroyer worm. This worm was used during the 2018 Pyongchang Olympics in South Korea. The worm temporarily shut down some South Korean IT systems ahead of the Opening Cermonies and brought down the Olympics website so people were unable to print tickets. According to Kapersky,

> "…the real interest of the cybersecurity industry lay not in the potential or even actual damage caused by the OlympicDestroyer's attacks, but in the origin of the malware. Perhaps no other sophisticated malware has had so many attribution hypotheses put forward as the OlympicDestroyer. Within days of its discovery, research teams worldwide had managed to attribute this malware to Russia, China and North Korea, based on a number of features previously attributed to cyber-espionage and sabotage actors allegedly based in these countries or working for these countries' governments."

---

62 Segal, Adam The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York, New York: Public Affairs, February 2016).

Upon further analysis, however, Kapersky found a 100% match in some of the OlympicDestroyer's coding to malicious software developed by a group called Lazarus, a nation-state backed group with links to North Korea. However, the 100% match was suspicious to researchers at Kapersky and, after more research into Lazarus' past behaviors, tactics, techniques, and procedures (TTPs) the cybersecurity agency found reason to believe that the portion of the code that matched Lazarus-developed software was intentionally placed within the worm to mislead forensic analysts.

"To our knowledge, the evidence we were able to find was not previously used for attribution. Yet the attackers decided to use it, predicting that someone would find it. They counted on the fact that forgery of this artifact is very hard to prove,"[63] said Vitaly Kamluk, head of the APAC research team at Kaspersky Lab.

He continues, "It's as if a criminal had stolen someone else's DNA and left it at a crime scene instead of their own. We discovered and proved that the DNA found on the crime scene was dropped there on purpose."[64]

While the accurate attribution of the OlympicDestroyer attack is still under debate, it is possibly the first example of a false flag deception technique being used to manipulate evidence. Despite OlympicDestroyer's sophisticated deception techniques, it was still found out by cybersecurity firms. However, like many cyber operations techniques, cyber deception

---

63 Bettencourt, Jessica "The Olympic False Flag: Infamous OlympicDestroyer Malware Designed to Confuse Cybersecurity, Community," Kapersky Labs, March 2018, https://usa.kaspersky.com/about/press-releases/2018_the-olympic-false-flag.

64 Ibid

is still in its relative infancy and one can expect these deception techniques to increase in complexity and effectiveness as more attempts are made and tactics become more refined.

Attribution: Geopolitics

Some authors claim that, while global connectivity allows for the possibility of ultimate digital freedom of movement and anonymity to mask attacks, geopolitics will still drive who attacks who and can provide circumstantial evidence to help in attribution.[65] In other words, even though it is possible for a Russian agent to use, for example, a German based IP address to commit DDOS attacks against Ukraine, geopolitics will still narrow down who would want to conduct such an attack against the victim. It is much more likely that Russia would want to shut down Ukrainian government sites than Germany would. So, while ultimate freedom of movement can provide full anonymity in theory, in practical reality it is not often achieved and there are enough markers in the attack design to help find some level of attribution.[66] While anonymity in cyber attacks is theoretically possible, it is not a guarantee.

Just War, and the Gray Zone

The last aspect of cyber operations to analyze before looking at how revisionist powers have implemented it is whether cyber attacks legally count as an act of war and what

---

65 Valeriano, Brandon & Maness, Ryan *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, New York: Oxford University Press, 2015).

66 Rowe, Neil "The Attribution of Cyber Warfare," in Cyber Warfare: A Multidisciplinary Analysis (New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

place cyber operations have in international law. This is important because legal ambiguity is an effective trait of gray zone operations—which will also be defined in this section.

There are multiple arguments that have been made advocating for cyber attacks to be classified by the UN as an action that warrants armed physical response. Most common is the argument concerning the UN's prohibition on the use of force.

UN article 2(4) states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in other manner inconsistent with the Purposes of the United Nations."[67]

This article is referred to as one of the cornerstone provisions of the UN as an organization. There are other places in the UN charter that provide exceptions to this rule, such as Articles 51 and 39-42 where use of force is authorized in self-defense and under UN specific authorization respectively. Outside of those articles of exception, it is generally unauthorized for one state to use "force" on another state legally according to both the UN and customary international law.[68]

Applying cyber operations to this article is difficult for several reasons, according to Green. It does not help that the UN charter was written decades before any idea of cyber operations would come into practice. The first argument that Green cites is the definition of "force". If it can be agreed upon that force is defined as acts that violate "the territorial

---

67 Green, James "The Regulation of Cyber Warfare Under the *Jus ad Bellum"* in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

68 Ibid

integrity or political independence of any state…" as stated in article 4(2), then certain types of cyber attacks may fall outside that definition and do not violate territorial integrity or political independence. This is especially true since cyber attacks by nature often occur remotely and do not involve any physical incursion into another state's territory, thus compromising their territorial integrity and the fact that the internet as a whole is not considered a part of any state's sovereign territory. One could argue that a piece of hardware (or digital information) that belongs to a state is considered the territory of said state and therefore unwanted or non-condoned manipulation of that property constitutes territorial violation. This would be an unprecedented definition of territorial integrity, however.

An opposing argument would be that the article assumes an all encompassing definition of force that does include cyber operations. The final section of the article must also be taken into account, "…or in any other manner inconsistent with the Purposes of the United Nations." It can be understood that this section of the article is a catch-all for any force of one state against another.

This does not automatically place cyber attacks within the realm of prohibited action, however, for there are some who argue that cyber attacks should not be considered "use of force" to begin with. For instance, if cyber operations count as use of force, then what about economic actions or other forms of soft power moves against a state? Proponents of this latter argument claim that the UN article only applies to "armed" force in any form.

An issue arises here as well, however, because there are multiple other sections of the UN charter where "armed force" is specifically named—such as in the Preamble and certain

articles within Chapter VII. If armed force is specifically mentioned in certain parts of the UN charter, then "force" as used in article 2(4) without the word "armed" should be a broader, all encompassing term to include unarmed force.

More theorists go further and further into this legal debate of interpreting Article 2(4) both for and against including cyber operations into the prohibition, even going as far as looking at the overall mission and purpose of the UN and whether it was founded solely to reduce armed, military conflict or all forms of dispute between states. At the time of this writing, such arguments have proven inconclusive.

There have actually been several states that have made appeals to the UN under article 2(4) against economic and political action taken against them. Such states include Brazil, Ecuador, and Iran. All such proposals have been rejected. Therefore, history and precedent has concluded that soft power acts such as economic and political coercion do not count as illegal use of force while armed conflict definitely is. Cyber operations, however, have no precedent nor clear place within this article.

Legal issues aside, what matters more is the precedent set both by states conducting cyber attacks and the response from the international community. After all, historical precedent and the reality of international actions determine common international law more than legal interpretations. The fact is that nations have retaliated little when they fall victim to cyber attacks. The victim states have, at most, responded with soft power actions such as sanctions, federal indictments of specific individuals or companies (such as China's Huawei) associated with the attack. It is possible that they retaliate with cyber operations of their own

as well. However, these responses seem to have done little to deter or punish a state. Lack of solid evidence as discussed in the previous section only help to water down the impact of public accusal and retaliation.

Until something fundamental about cyber operations changes—such as a more solid means to apply attribution, establishment of new laws, or a significant increase in the damage done by cyber operations—then the precedent for international custom has been set. According to this newly established custom, cyber operations in their current form do not qualify as a violation of the UN charter and do not warrant armed response or hard power retaliation. This gives the green light for revisionist powers to continue conducting cyber attacks with little fear of reprisal.

The Gray Zone

The characteristics of cyber operations discussed thus far make it an ideal tool for the realm of inter-state interactions referred to as the gray zone.

"Actions in the gray zone break, ignore, or diminish the rules-based international order. Sometimes they violate international law; other times, they push at the edge of international law."[69] For this reason, there is not much use in a state appeal to the UN after falling victim to a gray zone tool. This is because the gray zone tool either falls short of breaking international law (such as cyber operations under Article 2(4)) or, the tool does

69 Dubik, James, Lt Gen, (U.S. Army, Ret.) & Vincent, Nic "America's Global Competitions: The Gray Zone in Context," Institute for the Study of War, (February 2018).

violate international law but the state uses it sparingly or defiantly, calling the bluff of the international community.

It is easy to see how well cyber operations fit into this paradigm. As seen earlier in this study, attribution for cyber attacks tend to be circumstantial at best and the impact of the attacks are typically limited in scope—not as violent or showy as physical attacks though the effects can sometimes be similar. It has also been seen through the analysis of Article 2(4) of the UN charter that cyber operations do not violate territorial integrity; the amount of legal ambiguity that exists in international law regarding cyber attacks further makes cyber operations lucrative for a state that bases their operations on bending the rules in order to deter retaliation. Analysis provided in this thesis of the character of cyber operations, international law, and the nature of the gray zone all indicate that state sponsored cyber operations are an ideal tool for revisionist powers who want to maximize their effectiveness in using the gray zone to subvert the current global order and achieve their own strategic goals without risk of retaliation. Now, this thesis will look into specific examples of how these revisionist powers have used cyber operations in an effort to identify their methods of operation and TTPs.

PART THREE: GEOPOLITICAL ANALYSIS

Russia

Russia's modern cyber operations history begins with their actions in Estonia in 2007. This was followed up a year later with cyber operations in concert with physical military acts in Georgia. In 2014, Russia followed a similar tactic in Ukraine including a SCADA attack and, most recently, utilized advanced information operations and manipulation of social media engines to interfere with US elections in 2016. In addition to the idea of reflexive control, another common theme throughout these cyber operations is Russia's doctrine of blended cyber and information operations. This concept will now be analyzed followed by a chronological look at Russia's progression in cyber use from Estonia to the 2016 US Presidential election. By understanding Russia's tactics in cyber operations, one can map the revisionist grey zone pattern that Russia is using, predict their future goals, and make a plan of action to deter them from threatening US interests.

Blended Cyber and Information Operations

Russian cyber operations are unique in that they blend network intrusion and attacks with information warfare. According to the US director of National Intelligence, Gen. James Clapper, Russia established a Cyber Command to conduct: "offensive cyber capabilities including propaganda operations and inserting malware into enemy command and control

systems. Russia's armed forces are also a specialized branch for computer network operations."[70]

According to Russian military doctrine, both cyber operations and information operations (IO) fall under the term "informatsionoye protivoborstvo" (IP) or "information confrontation" also known as Information Warfare (IW).[71] While Russia has used non-cyber information operations as early as 1999 against Chechnya, the two concepts of cyber and IO are married together in Russian military doctrine and are fully integrated into modern military campaigns.[72] This has been true with Russian military operations in Georgia and Ukraine. However, Russia has also been unafraid to use their information confrontation doctrine independent of military operations, as will be seen in the analysis of Estonia and the 2016 US elections.

Political Warfare

Russia's concept of cyber operations is based on a modern application of Clausewitz's writing on how states operate in times of peace. This modern application is commonly called "political warfare". According to George Kennan:

---

70 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

71 Jaitner, Margarita "Russian Information Warfare: Lessons From Ukraine," *NATO Coorperative Cyber Defense Center of Excellence*, (2015).

72 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

> "Political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures, and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."[73]

Thus, while actual cyber operations are relatively new, Russia has used this new tool and integrated it organically within a blended information warfare and military doctrine that has existed since the Soviet period.

Estonia

The Russian cyber attacks on Estonia are generally regarded as the first ever major cyber conflict. Relations between Moscow and the Estonian government had deteriorated in 2007 due to Estonia announcing its intentions to move a memorial statue of a World War II Soviet soldier—commonly known as the Bronze Soldier—from the capital, Tallinn, to the city outskirts.

While this act angered ethnic Russians living in Estonia, the emotions and political anger revolving around the proposed move of the statue stemmed from much deeper roots. As a natural borderland between Russia and rest of Europe, Estonia has gone back and forth between Soviet occupation, independence, and Nazi invasion in the past 100 years. As a

---

73 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

result, the nation's population contained a blend between Estonians who viewed the statue as a symbol of Soviet occupation and ethnic Russians who viewed the proposed move of the monument as an insult to the 27 million Russians who died during the war.

Estonia's decision to move the monument was not only a solution to smaller, practical issues of public-order in the city (removing a site of tension and clashes between ethnic groups) but it was also a symbol of Estonia's efforts to move outside their historical Soviet shadow and Russian sphere of influence to become more European. Shortly after Estonia proposed the plan to move the statue, Moscow made known its displeasure by exerting diplomatic pressure, threatening a boycott of Estonian goods, and issuing general warnings of serious consequences to the Russian-Estonian bilateral relationship.

The day before the proposed move of the statue, there were protests of up to 1,500 people. The protests quickly turned violent and approximately 300 people were arrested. The protests revolving the move of the Bronze Soldier are cited by Estonian officials as the "worst since the country declared its independence from the Soviet Union…" according to the Council on Foreign Relations.[74]

The cyber attacks began the night following the protests—hours before the move was scheduled. The attacks consisted of defacement of multiple government websites, a fake letter of apology from the Reform Party (lead political partner in the coalition government)

---

74 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

for moving the statue, and the overload of the Estonian parliament's email servers with spam, forcing a temporary shut down in email communications.

The cyber attacks that night were only the first wave. A few days later, the attacks increased in intensity and sophistication. DDOSes utilizing computers from all over the world shut down more Estonian websites including news outlet *Postimees Online.* The attacks culminated on 9 May, the same day Russia was officially commemorating the end of World War II. On that day, up to fifty-eight Estonian websites were down at any one time and Estonia's largest bank, Hansabank, had their online services shut down intermittently for hours at a time between 9 and 10 May. Eventually, the Estonian government shut down all external internet communication in defense. According to the Council on Foreign Relations, "The internet within Estonia was accessible, but Estonians living abroad were cut off from their bank accounts and news services." The cyber attacks finally ceased on 18 May at 11pm local (midnight, Moscow time).[75]

In the midst of the cyber attacks, the Russian government initiated a litany of soft power moves and public outcry: instituting sanctions on Estonia and demanding a revision of its laws concerning Russian minorities living in the country. Russia also accused Estonia of being a fascist regime and allegedly organized violent demonstrations both in Estonia and Russia, using groups such as Nashi (a Russian youth organization created by the Putin regime) to protest at the Estonian Embassy in Moscow. On 9 May, the same day that the

---

75 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

cyber attacks culminated, Russian President Vladimir Putin had publicly stated that those who "defile the monuments to the heroes of this war are insulting their own people and spreading enmity and new distrust between countries and peoples." Despite Russia's explicit public disapproval and smear campaign of Estonia's action, all of the cyber operations against Estonia were conducted by proxy groups and botnets spread across the globe that allowed the Russian government freedom from attribution of the attacks.[76]

There are several key characteristics of the attack on Estonia that should be noted. First, the attacks were preceded by other forms of soft power threats. Second, the attacks were committed by groups or lone hackers that the Russian government could claim plausible deniability from. Third, while disruptive, the attacks on their own ultimately caused no permanent physical damage nor territorial compromise and, in fact, the first order effects of the attacks (mainly the disruption in communications and defacement of websites) only lasted for several hours, falling below the threshold of war; in other words, Estonia made a quick, full recovery from the cyber attacks. Lastly, the attacks were a part of a larger information campaign, often paired with public statements such as that observed by President Putin on the same day as the climax of the attacks.

These four characteristics fall perfectly in line with typical gray zone tactics and, when viewed not as a lone incident but instead grouped with Russia's next attacks on Georgia and Ukraine, indicate a larger pattern of revisionist efforts to increase Russia's

---

76 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

sphere of influence into Europe without inciting a war. Russia's actions against Estonia made a significant geopolitical statement at relatively low cost, risk, and damage thanks to the use of proxy groups (although Russian officials have been documented stating the government's involvement in directing the attacks, though not conducting it themselves)[77] and avoidance of physical damage. As such, retaliation against Russia was viewed as "not worth it" by both the victims and the international community.

There are two additional factors of note regarding the attack on Estonia that must be analyzed. First is Estonia's unique dependance on networked technology. In 2007, the nation had quickly become one of the first countries to rely on networked technology for vital government and financial functions.[78] Second is the fact that the attack on Estonia may have actually been a trial run for Russia to test new cyber tactics before conducting larger, future attacks. There are several indicators in Russia's subsequent cyber use against Georgia and Ukraine that posit a high likelihood that Russia was using Estonia as a test bed to establish methods of integrating cyber into their military doctrine and use it as a tool to deter NATO and EU expansion in the region.

Estonia embraced technology shortly after its secession from the Soviet Union in 1991. Following the country's secession, Estonia was faced with the obstacle of trying to thrive as an independent country but lacking significant of physical communications

---

77 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

78 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

infrastructure and only half of its population having phone lines. However, this also proved to be a benefit for the country; deciding to use the internet to resolve their shortcomings, they were able to begin building from scratch as opposed to trying to update and recycle legacy technologies that other, more established nations of the time stuck with.[79]

An additional factor pushing the country towards early cyber dependance was the population's IT knowledge base. Estonian workers played a major role in the Soviet Space program and Telegraph Agency. Tallinn's Institute of Cybernetics, founded in 1960, provided the necessary educational foundation for many of the former Soviet workers. The technologically educated population combined with the lack of infrastructure pushed the Tallinn government to begin initiatives for the country to become one of the world's first "information societies".[80]

All Estonian schools had regular online access by 1998 and the country declared internet access a human right by 2000. This declaration would be the first for any government in the world (find citation in HWO if this is really true). The government's cabinet went completely paperless and, in 2001, it became a national standard to issue ID cards equipped with digital signatures to Estonian citizens.[81]

By 2007, the same year as the cyber attacks, 95% of bank transactions were conducted on the internet (remember that Estonia's largest bank had its services completely

---

79 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

80 Ibid

81 Ibid

stopped for periods as long as 90 minutes during the attacks), health forms were stored on the digital cloud, and voting and income tax filing (both of which require access to Estonian government sites) were conducted online. This heavy use of online services for critical infrastructure and communications made Estonia a lucrative target for any nation hoping to see what impact cyber attacks could have on a society.[82]

The very next year, Russia used very similar cyber tactics in Georgia, this time in conjunction with real world military actions. Based on what appeared to be newly developing Russian cyber tactics, techniques, and procedures (TTPs), some theorists postulate that the Russian cyber operations in Estonia were a test run to see how a nation (and the rest of the world) would react to such information warfare. The apparent success in disrupting Estonia's daily operations while steering clear of international condemnation and serious retaliation was a green light indication for Russia that their tactics were a feasible option as a gray zone tool.

Estonian authorities postulate that Russia's larger objective in 2007 may have been to use their cyber influence to incite violent civil unrest between Estonians and ethnic Russians. This violence would have given the Kremlin justification to step in with physical action to protect pro-Russian factions, possibly even annexing part of Estonia. This plan is very

---

82 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

similar to what Russia has done in Ukraine. In fact, this methodology is an exact example of Russia's "Reflexive Control" strategy.[83]

Georgia

As stated, Russia's cyber attacks in Georgia incorporated the tactics seen in Estonia, but were implemented into a larger scheme of maneuver organically tied to physical military operations.

South Ossetia was the focal point of the conflict—a semi-autonomous area that already had a tenuous relation between Georgia and Russia. In the mid-2000s, South Ossetia had voted for full independence from Georgia and also had intentions of joining NATO.[84] In 2008, South Ossetian and Georgian forces exchanged gunfire with over 8,000 Russians conducting military exercises just across the border.[85] The fighting peaked when Georgian forces made it to the Ossetian capital, which triggered a Russian military response. After Russian forces pushed all the way to the Georgian capital of Tbilisi, Russia recognized Ossetia as an independent nation.[86]

While the conflict itself was short-lived, It carried a great amount of significance to Russia for two reasons. First, this conflict marked Russia as a power that was willing to

---

83 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

84 Ibid

85 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

86 Ibid

ignore international standards and institutions—by unilaterally using physical force and intervention, violating a nation's sovereignty—in order to achieve their own strategic objectives. Second, this was the first time Russia integrated offensive cyber operations into conventional, physical warfare.

Extremely similar to Estonia, Georgian government websites came under attack and were shut down. This happened shortly before Russian military troops began moving against Georgia.[87] Additionally, the website for the largest commercial bank in Georgia was taken down in conjunction with Georgian forums where local hackers might try to organize a defense or cyber counter attack.[88]

While most of the cyber actions were unsophisticated DDOS attacks and website defacement, these simple attacks were implemented in a very coordinated and complex way —in perfect timing with physical military maneuvers. The list of targeted websites skyrocketed at the same time that Russian troops established positions in Georgia.[89] The victimized sites included government agencies, financial institutions, business groups, educational institutions, news media, and a Georgian hacking forum. This was likely to prevent a coordinated Georgian government response and to increase the "fog of war." With the Georgian government limited in their ability to communicate to their citizens and the

---

87 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

88 Ibid

89 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

outside world, there was widespread confusion within the country. As soon as the physical military operations ended, so did the cyber attacks. Websites were later found that revealed online discussions of the upcoming military operations several weeks before the fighting actually started.[90] The near perfect coordinated timing between the physical and cyber attacks indicate that—even if the latter were conducted by non-government entities—the cyber attackers likely had access to the Russian military's tactical plans and list of targets.

Interestingly, Russia denied responsibility for the cyber attacks, despite their clear physical military involvement in the conflict. Beyond the geopolitical initiative, there was other evidence pointing to Russia's involvement in the attacks to include Russian terms in the malicious code and the term "win+love+in+Russia". This is all circumstantial evidence at best, however. Additionally, it is highly possible for the real perpetrator of attacks such as this to purposely insert clues into the code to mislead analysts into thinking that a certain nation was behind the attack—the false flag operations discussed earlier in this thesis.

Further complicating the issue of attribution, much of the coordination for these attacks were done in the public internet domain. Russian speaking websites such as "stopgeorgia.ru" distributed instructions on how to help with DDOS attacks against Georgian websites. Therefore, anyone in the world could contribute to the attack and the Russian government could claim no responsibility for the actions and information shared across a public website. Russia argued that, technically, anyone could be behind the attack.

---

90 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

This was an expert move on Russia's part. Not only did using the public domain make it harder to accuse the Kremlin of the attacks, it also shifted the focus to who Russia claimed was actually the source of the attacks—a disgruntled people looking for a way to speak out against unjustness. The topic of international conversation turned from accusing Russia of being behind the attacks to a discussion on expression of free speech. Russia argued that cyber attacks were simply another way for the public to speak out freely.

One piece of convicting evidence, however, pointing to government involvement, was the fact that "stopgeorgia.ru" published a comprehensive list of digital targets for DDOS attacks mere hours after the Russian military advanced. The cyber attacks simply seemed too well coordinated with the military operations to have been planned entirely in a vacuum. Still, the evidence was circumstantial at best.

Finally, Russia's IO campaign extended beyond the typical cyber attacks aimed at shutting down government services and sites. Russian bloggers manipulated a CNN-Gallup poll, filling the site with comments that tried to justify Russia's cause and overwhelm any pro-Georgian posts or comments.[91] Different from DDOS attacks and other forms of cyber attack, publicly posting opinions on social media and news sites is perfectly legal and there was little way to prove whether the source of the posts was the Russian government or just opinionated Russian citizens. There are major similarities between the CNN-Gallup poll posts and the social media propaganda flood that Russia used during the 2016 US

---

91 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

Presidential election. These similarities could indicate that Russia was experimenting with social media influence as far back as 2008 and had a more refined tactic by the 2016 elections.

What was Russia's geopolitical goal in the attacks on Georgia? To prevent Georgian accession to NATO and demonstrate Russia's dominance in the region. Not only did Russia's combined IO and IW campaign significantly contribute to that cause, it allowed them to achieve it without inciting a conventional war and set a precedent that Russia would maximize in future international disputes.

Georgia's defense against the attacks, while much better than Estonia's, bring up yet another interesting issue. While Estonia essentially defended their networks on their own and resorted to shutting down their external communications, Georgia relied on servers owned—and located within—other nations. Agencies within Poland and Estonia offered their servers to host the Georgian websites that were under attack so that they could still be accessed. US companies such as Google also offered up their server space.[92] [93] This brought up some potential international complications, because this act of assistance by US business were conducted without knowledge or approval of the US government. By offering an auxiliary for Georgian government communications, Google (and other smaller companies) effectively involved the US in the conflict. In fact, Russia's DDOS attacks followed Georgia's trail of

---

92 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

93 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

retreat and began attacking US servers.[94] This means that Russia was attacking Georgian government and banking websites hosted on commercial US servers in assistance to a Russian military advancement.

Estonia and Georgia: Factors Contributing to Attack Effectiveness

While the cyber attacks on Georgia were remarkably similar to that against Estonia, the short term effects were much different. There are two main reasons for this. First, Georgia was significantly less dependent on networked technology for critical communications than Estonia was. Second, Georgia was less technologically advanced and most of their physical cyber infrastructure ran through Russian territory.

Estonia and Georgia: Physical Infrastructure

Regarding the physical cyber infrastructure (the physical cables and nodes that carry the information both within a nation and across the world), Estonia had the benefit of being an internet exchange point (IXP). IXPs are nodes where multiple network carriers meet. By having an abundance of node intersections, Estonia was able to maintain internal communications while cutting themselves off from outside the outside world. Georgia on the other hand, did not have these physical luxuries and thus could not cut themselves off without also shutting down internal communications. In fact, most of Georgia's cyber infrastructure ran through Russia—giving them little control or power over communication

94 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

flow. This demonstrates that the physical layout of a nation's cyber infrastructure is an extremely important factor to plan for when it comes to both cyber attacks and defense.

Estonia and Georgia: Technological Reliance

The difference in technological reliance between Estonia and Georgia is a second good point of analysis that indicates a direct correlation between cyber attack effectiveness to the number of networked devices in the victim nation. As stated earlier, Estonia chose to be heavily dependent on technology very early in the digital age. According to the Council on Foreign Affairs, Estonia had 57 "digital users" for every 100 in 2007.[95] In 2008, Georgia only had seven.[96] Almost no Georgian government services like finance and energy were connected to the internet. While the attack on Estonia prevented many citizens from conducting bank transactions and conducting essential services with the government, this was not the case with Georgia. The main disruption that Georgia suffered was the interruption of internal government communications as well as the broadcasting official statements to the rest of the world during the attacks.[97]

The difference in impact of Russia's attacks on both nations help to inform the rest of the world on the effectiveness of cyber attacks. As a general rule, the more dependent a nation is on cyber networks to accomplish critical services, the more vulnerable they are to attack. For example, a nation like North Korea is much less vulnerable than a technocratic

---

95 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

96 Ibid

97 Ibid

population like Seattle or San Francisco. Additionally, as more cities and nations become dependent on technology, it is good to note that the more redundant the infrastructure is, the more resilient it will be against attack. Georgia's ability to shift its websites to auxiliary servers (despite their location in other countries), helped mitigate the impact. This is one way that nations can defend against cyber attacks in the future to minimize disruption of low level attacks.

Ukraine

Two years after the Georgian conflict, Russia adopted a military doctrine that described contemporary conflict as "intensification of the role of information warfare."[98] The doctrine further stated that a modern military should use information warfare to achieve political objectives without the use of a conventional military force. If a military force must be used, then information warfare should work to form a "favorable response from the world community."[99]

Russia's 2014 intervention in Crimea demonstrated this military doctrine and further refined Russian tactics in using cyber operations—in the form of information warfare—to augment physical military action. While Russia follows the same pattern in Ukraine as in Estonia and Georgia, Ukraine stands out because the conflict was far deeper, the violence was longer lasting and, (unlike in Estonia and Georgia) Russia actually attempted to annex

---

98 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

99 Ibid

Crimea—a much bolder geopolitical move. Lastly, the Ukraine conflict witnessed a successful SCADA attack.

The conflict originated with demonstrations against the pro-Russian Ukrainian government at the time and a coup that overthrew their leader, Viktor Yaukovych. Russia viewed these acts as the US and the West trying to gain influence on the Russian border by trying to manipulate the Ukraine into becoming a pro-Western state.[100]

As the fighting started, Russian actors conducted heavy information operations through every medium including the internet to influence the Ukrainian and international audiences' perception of events. This was met with significant retaliation not only from Ukraine but also non-state actors such as Anonymous—an independent hacker group. Ukrainian hackers disabled websites belonging to the Kremlin, the Russian central bank, and Russia's Foreign Ministry while OpRussia—a subgroup of Anonymous—attacked Russian business and government sites to include sites for the Russian Air Force and the Federal Drug Control Service of Russia.[101] Ukrainian actors were also able to hack into Russian Interior Ministry servers to view closed-circuit television cameras to monitor Russian troop movements and military hardware.[102]

---

100 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

101 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

102 Ibid

In addition to the IO campaign, a NATO study found that Russia had been conducting a cyber campaign dubbed "Operation Armageddon" which began in mid-2013. According to a US cybersecurity firm, Ukrainian officials and high-level targets received spear-phishing emails containing malware designed to gain information on Ukrainian military strategies[103] (a precursor to the spear-fishing tactics used against the Democratic National Convention in 2016). While these spear-phishing attacks occurred while Yaukovych was still in power, the timing lines up with Ukraine's public interest in the Ukraine-European Union Association Agreement, which Russia opposed. Yaukovych eventually decided not to sign the agreement, which helped spark the pro-West rebellion that ousted him.

Throughout the fighting, Russia's cyber tactics largely mirrored operations in Estonia and Georgia—until 23 December 2015.[104] On that date, three electric power distribution companies were shut down by cyber attacks. This disrupted power for over 220,000 customers.[105] Additionally, hackers launched a DDOS attack against call centers which prevented Ukrainian residents from calling and reporting the power outage. This attack on SCADA systems had real, physical effects much like the Stuxnet attack on Iranian nuclear facilities and was far more sophisticated than any cyber operations conducted in Estonia and Georgia.

---

103 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

104 Ibid

105 Ibid

The US Department of Homeland Security conducted an investigation revealing that the attacks were conducted remotely by exploiting legitimate credentials of Ukrainian operators. The attackers gained remote control of breakers at over 50 regional substations. According to the investigation, the attackers likely gained these credentials far in advance of the attack, which means they waited specifically until December of 2015 to execute.[106]

Why did Ukraine witness a cyber attack on their infrastructure when Georgia and Estonia did not and why did it occur so late in the conflict? Russia had the ability and means to conduct attacks on Georgia's energy infrastructure[107] but did not execute, whereas they did in Ukraine. Strategically, Russia may have conducted this SCADA attack in Ukraine in response to a similar attack led by Ukrainian nationalists and Crimean Tartars one month before. In this attack, the nationalists disabled electricity transmission lines to Crimea. They did this through conventional means (physically toppling the transmission towers).[108] This resulted in a Crimean power outage that lasted two weeks. It is possible that Russia decided that an attack on Ukrainian power infrastructure was an appropriate response to Ukraine's escalation of the conflict. While the effect of Russia's response (loss of power) may have been equal, the means of accomplishing the effect (a cyber attack on a SCADA system) was entirely new and demonstrates Russia's ability to deter an enemy (and even cause physical harm) through cyber means when Russia deems such an attack as appropriate.

---

106 Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

107 Ibid

108 Ibid

Elections

The final example of Russia's cyber use in interstate competition is the 2016 US Presidential elections. According to the Council on Foreign Relations and the FBI,[109] a group of hackers called Cozy Bear with links to the Federal Security Services of Russia (FSB) infiltrated the Democratic National Committee (DNC) and Republican National Committee (RNC) in 2015. The hackers were able to gather emails, donor rolls, and other information on these servers uncontested. The hackers also successfully used a spear phishing attack to gain access to John Podesta's (the chairman of Hillary Clinton's presidential campaign) email account. In 2016, a second hacker group known as Fancy Bear—with links to Russian Military Intelligence group GRU—was also discovered as having access to both parties' servers.[110]

Initially, the US viewed these hacks as state versus state espionage—something every nation does. US news services reporting on the hacks assumed the Russians wanted to understand the US political system along with strengths and weaknesses of the political candidates. These assumptions proved false when a third hacker personality called Guccifer 2.0 made released stolen internal DNC documents to journalists and Wikileaks.[111]

Wikileaks published the documents three days before the Democratic National Convention and unveiled strife and instability within the DNC regarding Bernie Sanders'

---

109 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

110 Ibid

111 Ibid

campaign. Another website called DCLeaks was quickly created and also began releasing DNC documents while news sources such as the *New York Times*, the *Washington Post* and others began sifting through the documents for news stories that embarrassed and undermined both the DNC and the Hillary campaign.[112]

As a part of Guccifer 2.0's public release, he claimed that the DNC hacks were conducted by a lone actor not associated with Russia. Most agencies suspected Guccifer 2.0 to be a front for Russian intelligence to take suspicion off from Cozy Bear and Fancy Bear. The documents that Guccifer 2.0 offered, however, appeared to have been edited on Russian computers and linguistic proof was found that indicated Guccifer 2.0 was a native Russian speaker.[113]

One month before the presidential election, the Department of Homeland Security and the Director of National Intelligence (DNI) formally accused and attributed Russia for the hacks, claiming that the hacks were designed to interfere with the US election process. Three separate cyber security companies also came into agreement regarding Russian attribution after analyzing the attacks and digitally monitoring the hackers that were suspected of being responsible. The US decided to expel 35 spies and sanctioned the GRU, FSB, four intelligence officers, and three companies that assisted the hackers.[114]

---

112 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

113 Ibid

114 Ibid

In addition to the DNC and RNC hacks, there was an extensive social media campaign conducted by Russia through an organization known as the Internet Research Agency (IRA).[115] This St. Petersburg-based group was founded in 2013 and has been a close ally of President Putin and Russian intelligence. The initial goal of this group in 2013 was to write blog posts, comments, memes, and videos supporting certain Russian government interests while criticizing opponents. In April of 2014, the group expanded their operations to include influencing US political issues through social media. This naturally led to the group attempting to influence US citizens in voting decisions during the 2016 Presidential campaign.[116]

The IRA flooded social media platforms with pictures, posts, and memes designed to criticize certain candidates while promoting others. This included the creation of several Facebook pages, groups, and false news sites whose articles would be shared and re-posted across the web. The IRA even went so far as to pose as American citizens and organize real world political rallies in major cities—coordinating with real US activists who did not know they were actually working with the Russian group.[117]

These US activists unwittingly provided deeper knowledge and strategies to the Russian based misinformation operators. For example, according to the US Justice

---

115 Jenkins, Tricia "What did the Russian Trolls Want During the 2016 Election: A Closer Look at the Internet Research Agency's Active Measures," War on the Rocks, May 2018, https://warontherocks.com/2018/05/what-did-russian-trolls-want-during-the-2016-election-a-closer-look-at-the-internet-research-agencys-active-measures/.

116 Ibid

117 Ibid

Department, the IRA made contact with a Texas-based activist who advised them to ignore firm red and blue states such as Texas and Vermont and to shift their efforts on "purple states" that could vote either way in the election.[118]

This type of information provided by unwitting US citizens about which states were worth targeting helped the IRA who lacked that type of intimate, insider knowledge on the US political system. According to the Justice Department, there was a noticeable change in the IRA's tactics and their spending habits on Facebook ads as the campaign progressed and the group gained more knowledge to fuel their methodology.[119] At the start of the campaign, the attacks lacked cohesion and clear direction. However, they became more focused, organized, and refined as the IRA gained more knowledge in how to efficiently target their ads and misinformation to audiences who would be most receptive to it.

So then, what were Russia's geopolitical goals in the US election hacks? According to the House Permanent Select Committee on Intelligence, the primary goal was to "sow discord in American society" and that Russia had no goals of supporting a specific candidate.[120] While Russia has actively supported fringe political parties and disparaged anti-Russian candidates in other countries in past elections, the House concluded that this was not the case in the US elections. However, the Senate Intelligence Committee came to a

---

118 Jenkins, Tricia "What did the Russian Trolls Want During the 2016 Election: A Closer Look at the Internet Research Agency's Active Measures," War on the Rocks, May 2018, https://warontherocks.com/2018/05/what-did-russian-trolls-want-during-the-2016-election-a-closer-look-at-the-internet-research-agencys-active-measures/.

119 Ibid

120 Ibid

seemingly different conclusion. According to the Senate, the Russian hackers specifically had goals to support President Trump and disparage Clinton.[121]

Research teams and independent analysts have stated that the two different objectives stated by the House and Senate are not mutually exclusive. While there is evidence indicating the IRA's support of president Trump, there is also evidence of support for Bernie Sanders and as well as attempts at general confusion and distrust in the American political system. Either way, it appears that both objectives were met, regardless of which one was Russia's true intent.[122]

Russia's hacks on the US presidential campaign demonstrated a new level of Information Operations. It was the manifestation of their 2010 military doctrine that described contemporary conflict as "intensification of the role of information warfare" and stated that a modern military should use information warfare to achieve political objectives without the use of a conventional military force. Rather than DDOS attacks and website defacement like in Estonia, Georgia, and Ukraine, Russia was able to utilize much more complicated and subtle misinformation tactics that started with espionage and theft followed by using the information gained to shape the news, media, and online landscape to influence US citizens. This misinformation even resulted in physical actions with political rallies being formed.

---

121 Jenkins, Tricia "What did the Russian Trolls Want During the 2016 Election: A Closer Look at the Internet Research Agency's Active Measures," War on the Rocks, May 2018, https://warontherocks.com/2018/05/what-did-russian-trolls-want-during-the-2016-election-a-closer-look-at-the-internet-research-agencys-active-measures/.

122 Ibid

The organization of political rallies serves as a disturbing proof of concept. If Russian online personas were able to organize offline, real world political rallies, it would not be a far leap for these Russian entities to organize riots, protests, or even violent actions purely through online influence. In fact, this has already been done in the past with non-state actors. The Islamic State in Iraq and Al-Sham (ISIS) has extensively used social media to spread their ideology and influence violent "lone wolf" attacks across the globe, often providing instructions on how to conduct these attacks.[123] The difference with Russia, however, is their subtlety. They have proven capable of organizing a physical presence to achieve their geopolitical goals without the organizers and participants knowing that they were being influenced by a foreign state power. This is a clear achievement of their contemporary military doctrine of using information operations to achieve political objectives without the use of physical military action.

China

China is the second revisionist power that has heavily used cyber operations to gain strategic interests and destabilize the global status quo. A look at how China has implemented cyber operations, however, will show some fundamental differences in their tactics. Where Russia uses misinformation, subversive use of social media, and cyber operations organically paired with forms of soft power and even physical military action, China utilizes a more subtle approach of data theft, corporate espionage, and Advanced Persistent Threats (APTs).

---

123 Celso, Anthony "The 'Caliphate' in the Digital Age: The Islamic State's Challenge to the Global Liberal Order," *The International Journal of Interdisciplinary Global Studies*, Volume X, Issue X, (2015).

Also worth analyzing are China's heavy cyber defenses and controls on networked access courtesy of their "Great Firewall" and "Great Cannon."

China's Two Sided Cyber Doctrine

China has a very dual-sided view of the internet. First, they see it as fundamental to economic growth and in keeping up with the rest of the world. On the other hand, however, the government also sees the internet as a vulnerability that allows Western influence to reach in and create unrest among the country.

In a white paper published in 2010,[124] China described the internet as having an "irreplaceable role in accelerating the development of the national economy." The paper also discussed its valuable use in supervision and quick dissemination of information from the government to the people. China has a centralized social media platform called Weibo that allows the government to see what issues the populace are discussing and can then disseminate information appropriately to maintain order.

However, another paper—this time published by the *People's Liberation Army Daily* in 2015—states that,

> "Foreign forces use this convenient tool of the internet to build 'value traps,' implement a 'cultural cold war,' and foster 'a fifth column,' befouling leaders, vilifying heroes, mocking the system…[A]ttacks against the army may be said to

124 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

have reached a state of unbridled brazenness, making the Internet into 'concession' to peddle Western ideology."[125]

This perceived ideological threat from the West has caused China to create a comprehensive cyber defense which is colloquially called the Great Firewall of China.

China's First Political Objective: Defense and the Great Wall of China

The Great Firewall is a combination of technologies that filter and block material originating from outside of China that is deemed offensive or a threat to the Chinese government. In addition, the Great Firewall has several inward looking tools that censor content generated within the country. In addition to filtering for offensive content, the Great Firewall is also used to block malicious code that would attempt to attack computer systems.[126]

China has been very public in favoring a controlled internet over an open one. The head of the State Internet Information Office—which regulates the nation's internet—further defined China's stance, stating that China was hospitable to western websites but should also be able to, "Choose who can come to our home and be our guest. I can't change who you are but I have the power to choose my friends. I wish that all who come to China will be our real friends."[127]

---

125 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

126 Ibid

127 Ibid

China's role in controlling the internet does not end with passive filtering and blocking of content, however. The nation also has an extensive history of hacking companies and websites who exist outside the country. Their public purpose for doing this is to stop—at the source—any entity who may be an online threat to the government's control over its people.

For example, China has another national cyber tool called the Great Cannon, that is capable of creating severe cyber attacks. The Great Cannon allows China to intercept foreign web traffic inbound to the country, inject malicious code into the transmission, then redirect the traffic elsewhere.[128] The world discovered this new capability in 2015 when China caused the website Github to crash. GitHub is a popular website for programmers to post source code free for use by the public. A nonprofit organization had used the site to publish a program that would allow Chinese web users to circumvent the Great Firewall. Seeing this as a threat, the Chinese government used their Great Cannon to shut down the website for five days.[129]

China's Great Firewall, Great Cannon, and cyber attacks in the name of defense and censorship constitute only one aspect of their cyber doctrine. China's cyber capabilities discussed up to this point are only designed to help the country shape the internet into a more favorable environment. This thesis will next discuss the next aspect of China's cyber doctrine

---

128 Valeriano, Brandon & Maness, Ryan *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, New York: Oxford University Press, 2015).

129 Ibid

—espionage, data theft, and advanced persistent threats designed to give them an edge in achieving regional political adjectives without resorting to physical acts of war.

China's Second Political Objective: Economic and Military Competition

As stated earlier, China's view of the internet is twofold. It is an avenue for dangerous outside influence as well as for economic prosperity. For the former, China's solution is the Great Firewall and cyber attacks conducted for the purpose of crafting a favorable internet. When it comes to economic prosperity, however, the country has resorted to data theft and corporate espionage.

In addition to giving Chinese companies an edge against foreign competition, this espionage gives the same added benefit to the Chinese military—allowing them to see what the US defense industry is working towards in order for the Chinese to keep up.[130] China has stolen military data on over two dozen Department of Defense weapons programs including the Patriot missile system, the F-35 Joint Combat Fighter, and the Littoral Combat Ship—the US Navy's new category of surface warships.[131]

While spying on adversary military capabilities is standard operations for most countries, this is especially important for China. Chinese defense spending is less than one-

---

130 Brown, Ian "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust," War on the Rocks, May 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/.

131 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

fourth of the US[132] and, while the US military has been actively engaged in combat nearly consistently since the turn of the century, the Chinese military is largely untested. China fears that their military will not be able to stand up to a conflict with the US and thus relies on extensive espionage to compensate.

There are multiple regional hotspots that China is involved in where they fear US intervention: Taiwan, the South China Sea dispute, and Chinese Naval expansion into the South Pacific. In order for China to deter the West from intervention—or, worse, avoid a loss should a military conflict arise—the nation resorts to cyber espionage to give the every competitive edge possible against US military capabilities and development.[133]

While examining every instance of Chinese cyber attacks, espionage, and data theft would not be feasible in the scope of this paper, this thesis will examine a few key operations that indicate China's successful use of cyber operations to achieve their political objective of economic and military competition.

Titan Rain

China's first notable data theft attack was discovered in 2003 by a network administrator for Sandia Labs. On investigating a data breach on a Lockheed Martin facility in Florida, he discovered that computers in China were in possession of a complete network

---

132 Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

133 Brown, Ian "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust," War on the Rocks, May 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/.

scan report of Ft Dix—a US Army Post located in New Jersey. The next year, the same network administrator discovered that the same attackers from before had obtained hundreds of documents belonging to multiple US research and military facilities—this time including the Defense Contract Management Agency and the World Bank.

These two discoveries, coupled with several others being researched by the FBI, were collectively given the name “Titan Rain.” This attack stands out because it raised awareness for the threat of Chinese data theft and identified a new type of cyber attack called an “Advanced Persistent Threat” or, APT.

Lockheed Martin describes APTs as targeted, coordinated, and purposeful cyber attacks that operate for a prolonged period of time (months or years) against a target with intent and opportunity.[134] Most of China’s cyber attacks have these traits and are often only discovered after the malicious program has been siphoning off data from a specific target for months or even years.

APT10 2006-2018 Hacks

While china has a very extensive list of corporate hacks that have resulted in the theft of intellectual property both in the private and military sector, perhaps one of the longest running APTs was discovered in December 2018. In that month, US officials indicted two Chinese nationals who were identified as members of a group known in the cyber security

134 Hutchins, Eric "The Cyber Kill Chain,” Lockheed Martin, 2019, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

community as APT10—a hacking group acting on behalf of the Chinese Ministry of State Security.[135]

These two individuals were charged for involvement in a hacking campaign that had started in 2006.[136] By 2018, dozens of companies around the world along with several US military agencies were compromised to include the US Navy, NASA, Hewlett Packard, IBM, and several companies "involved in aviation, space and satellite technology, finance, electronics, healthcare, oil and gar exploration" according to a Reuters report.[137] FBI Director Christopher Wray stated, "The list of victim companies reads like a 'Who's Who' of the global economy".[138]

According to the FBI director, "No country poses a broader, more severe long-term threat to our nation's economy and cyber infrastructure than China…China's goal, simply put is to replace the US as the world's leading superpower, and they're using illegal methods to get there."[139]

---

135 Greenfield, Charlotte "New Zealand Intelligence Agency Joins Allies in Blaming Chinese Government for Hacking," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-newzealand/new-zealand-intelligence-agency-joins-allies-in-blaming-chinese-government-for-hacking-idUSKCN1OJ2M1.

136 Bartz, Diane & Stubbs, Jack, "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies-idUSKCN1OJ1VN.

137 Ibid

138 Ibid

139 Ibid

It is clear, then, that China's cyber espionage attempts are specifically targeting two categories of industries: 1. Industries where stolen intellectual property would give Chinese firms a competitive advantage (science, engineering, and technology), 2. Military infrastructure in order to give the Chinese military knowledge of the US military's capabilities.

In addition to those above two categories, however, exists a third target—information that would prove useful for counterintelligence purposes. Among all the data that was stolen were the Social Security numbers of more than 100,000 US Naval personnel.[140] This was far from the first time that personnel data of US citizens—specifically US government workers—were compromised. Two other major data breaches involved the Office of Personnel Management and the Marriott hotel chain. These two data breaches will now be discussed to demonstrate how China is achieving their third political objective through cyber attacks—a counterintelligence advantage over the US.

China's Third Political Objective: Counterintelligence

In July of 2014, the media reported that Chinese hackers had compromised servers belonging to the Office of Personnel Management (OPM). OPM is responsible for the personal information of tens of thousands of federal employees. Specifically, OPM maintains

---

140 Bartz, Diane & Stubbs, Jack, "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies-idUSKCN1OJ1VN.

security investigation paperwork for every individual who has access to classified information—including military and intelligence personnel.[141]

The security investigation documents that the Chinese gained access to included what is known as a Standard Form 86. This form is filled out by every individual applying for a security clearance to access classified information. Beyond basic personal information such as Social Security numbers, data on this form includes disclosure of financial trouble, alcohol and drug history,[142] as well as other very private information such as a list of close friends from every address the individual has lived sometimes up to ten years prior to the date of the application. For example, a federal employee who is filing the paperwork for a security clearance at the age of 22 years old would have to document on that form every place they have lived along with close friends who knew them at each address starting from the time they were 12 years old.

There exists significant speculation as to what the Chinese could do with this data—everything from blackmailing US government workers to tracking down and arresting clandestine intelligence officers working abroad. Regardless of what counterintelligence actions China could take with this information, the data gained has certainly given China a comprehensive picture of nearly every US federal employee and official. The information from the OPM data breach provides China with a groundwork on which they can connect

---

141 Brown, Ian "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust," War on the Rocks, May 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/.

142 Ibid

other personal data to—such as the case with the 2018 data breach on the Marriott hotel chain.

In 2018, Marriott announced that hackers had gained access into the company's reservation system. Initially, it was dismissed as a case of criminals trying to steal financial data such as credit card information. However, the hotel chain discovered that the hackers had gained access as early as 2014 and maintained persistence for years, gaining information on over 500 million customers.[143] For hackers to stay inside a system for that long is an unusual method of operations for criminals looking for financial gain. This extended access was consistent with Chinese APTs, though, and the tools used to gain access were the same ones implemented in previous data breaches also attributed to the Chinese.[144]

The hack was also initiated shortly after the OPM hack had been publicly announced. Therefore, it is possible that, after discovery of the OPM breach, China began looking for other avenues to gaining private information on high interest US individuals.[145] As the world's largest hotel operator—owning Starwood, the Sheraton, Westin, and over 20 other hotel brands—Marriott has a high frequency of stays from US federal employees, officials, and military members traveling both for work and leisure.

---

143 Bing, Christopher "Exclusive: Clues in Marriott Hack Implicate China - Sources," Reuters, December 2018, https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D?mod=djem10point.

144 Ibid

145 Bartz, Diane & Stubbs, Jack, "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies-idUSKCN1OJ1VN.

While not as personal as the information gained from the OPM hacks, compromised Marriott data included names of travelers, passport numbers, address, phone numbers, birth dates, and email addresses. If China was, in fact, behind the data breach, they could pair hotel data with OPM records to track the travel movements of any government individual staying in a Marriott chain hotel—of which there are over 6,500 around the world including inside China.[146]

From a counterintelligence standpoint, China can track when two possible US intelligence members travel to the same hotel, possibly indicating a clandestine meetup. This would allow China to build a network map of intelligence members, their connections, and their movement patterns around the globe. They could place wiretaps in rooms where high interest individuals make reservations. They could also place their own Chinese foreign intelligence spies in the same hotel that a US individual with a security clearance is staying in. Using personal data from the OPM hack, that Chinese spy can then intercept the US individual and use human intelligence techniques to influence them to help the Chinese.[147]

The Marriott hacks were the first of its kind in a way. Up until that point, it was widely known that China was stealing data to give their own military and companies and edge over their competitors. However, the idea of China stealing personal data en masse from

---

146 Bartz, Diane & Stubbs, Jack, "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies-idUSKCN1OJ1VN.

147 Brown, Ian "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust," War on the Rocks, May 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/.

businesses potentially for counterintelligence purposes is still a novel concept. The Marriott hacks were the first to indicate that this could be a potential Chinese tactic. As of the time of this writing, intelligence and security professionals are still identifying the potential vulnerabilities that this data poses to US government individuals.

Raiding

Looking at both Russia's and China's cyber actions together, another concept that helps provide context to their cyber operations is the idea of "raiding." As defined by geopolitical analyst Michael Kofman, "Raiding is the way by which Russia seeks to coerce the United States through a series of operations or campaigns that integrate indirect and direct approaches. Modern great power competition will thus return to forms of coercion and imposition reminiscent of the Middle Ages, but enacted with the technologies of today."[148]

In other words, raiding is the term for the act of a weaker power to execute surprising, short, high impact operations against a more powerful actor that cumulatively achieve a strategic objective. Historically, raiding was a concept used throughout Europe by small groups fighting against their stronger neighbors or kingdoms. In comparison to large scale military actions, raiding utilizes agile, fail fast and fail cheap operations consisting of quick execution. The Kofman continues,

---

148 Kofman, Michael "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," War on the Rocks, June 2018, https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/.

> "If war is not an option and direct competition is foolish in light of US advantages, raiding is a viable alternative that could succeed over time. Therefore, Russia has become the guerrilla in the international system, not seeking territorial dominion but raiding to achieve its political objectives…If Moscow can remain a strategic thorn in Washington's side long enough for Beijing to become a global challenge to American leadership, Washington may have no choice but to negotiate a new great power condominium that ends the confrontation, or so Moscow hopes."[149]

Historically, raiding is most effective against an opponent who possesses military overmatch but is distracted by a different threat. When traditional warfare is too costly, too risky, or unsuitable, raiding provides a concept within the gray zone for smaller individual operations to achieve, over time, a larger strategic goal.

Gray zone cyber operations are the modern day instruments of raiding. The idea of raids can be taken to help define the large number of small cyber operations that in and of themselves may not achieve much strategically but cumulatively have an impact—similar to the idea of death by a thousand cuts. China and Russia have conducted far too many cyber operations against not only the US, but other western state competitors to cover in within the scope of this thesis. However, when incorporating the idea of raiding, their individual operations can be viewed as achieving larger, organized strategic objectives that are slowly achieved through the many smaller attacks. When China's and Russia's cyber operations are

---

149 Kofman, Michael "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," War on the Rocks, June 2018, https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/.

viewed as operations executed in concert, the two revisionist powers achieve more together to bring down the US unipolar hegemony of the post Cold War era.

The Return of Nation-State Rivalry

In January of 2019 the Director of National Intelligence (DNI) issued the US Intelligence Community's annual Worldwide Threat Assessment. The very first statement made in the assessment directly after the Foreword is:

> "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure."[150]

The assessment then immediately discusses specifically the revisionist threat that China and Russia pose to the current world order. After cyber, the next threat discussed is online influence campaigns carried out against democratic processes. Terrorism and Islamic extremism take on a much smaller role in the article. This IC assessment makes it clear that

---

150 Coats, Daniel (Director of National Security), "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, (29 January, 2019).

nation-state rivalry has replaced terrorism as the biggest threat to the United States and that the biggest tool or method of conducting this rivalry is through cyber means.[151]

It is an interesting point to note that the assessment discusses these threats not as something to be eliminated or prevented, but instead as a new standard and regular occurrence in international affairs. This indicates that it is now commonly understood both throughout the Intelligence Community and international stage that state sponsored cyber attacks are not only commonplace, but physical retaliation against most types of attacks is unlikely. It is also understood that other forms of soft power retaliation such as indictments and sanctions are not expected to deter a state from conducting these attacks. The wording in this report confirms that revisionist powers have established a foreign policy TTP of turning to cyber operations when soft power actions are not achieving the desired national security or economic goal. This report has solidified the US belief that cyber operations are now the lead gray zone tool for states to achieve political objectives when traditional soft power tactics are not enough.

---

151 Coats, Daniel (Director of National Security), "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, (29 January, 2019).

What Cyber can and Cannot Achieve

The threat assessment breaks out the cyber threats into three components: influence operations, cyber attacks that cause physical damage, and cyber espionage.[152] Both influence operations and cyber espionage have already been discussed at length in this thesis. However, it is important to look at the potential and likelihood for cyber attacks to cause physical damage and the role that those types of attacks are predicted to play in this new inter-state competition.

The 2019 IC assessment states that both Russia and China are capable of disrupting critical infrastructure for a time period ranging from a few hours to several weeks. The assessment also states that Moscow specifically is mapping US infrastructure with the long term goal of causing substantial damage.[153] Additionally, experimental hackers at McAfee have demonstrated various ways that IoT devices can be manipulated by malicious actors. Their experiments have utilized everything from smart TVs to vehicles to WiFi enabled lights and smart speakers—manipulating them to cause physical damage or even possible harm.[154]

That being said, expectations on what cyber operations can and cannot be expected to achieve should be made. It is true that revisionist powers have advanced to a point where

---

152 Coats, Daniel (Director of National Security), "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, (29 January, 2019).

153 Ibid

154 Siskind, Geoff "Hackable Podcast by McAfee," McAfee, February 2019, https://hackablepodcast.com/.

they can do physical damage to infrastructure purely through computer network manipulation. In fact, McAfee's experiments show that even a lone actor can cause physical damage through cyber means.[155] However, these types of attacks are not the most likely future course of action for revisionist states conducting cyber operations. While cyber attacks are now commonplace, physical effects on the level of Stuxnet will still be the exception rather than the norm.

If states have the power to deal physical, violent damage to their opponents through cyber means, why would they avoid doing so? This is because cyber operations are most beneficial when used within the realm of the gray zone. The benefit of a cyber attack is that it is capable of temporarily disrupting critical infrastructure specifically without causing the same level of permanent destruction as a conventional military attack. This temporary disruption is something that physical attacks cannot do. Gray zone tools achieve political objectives specifically without having to resort to physical conflict. The goal of a gray zone tool is not to cause destruction to a state that is on the scale of a war, neither is it to provide a new way to wage traditional war. Rather, if a state wants to realize the full potential of gray zone cyber operations, they should be trying to achieve political objectives with the least amount of destruction possible in order to *avoid* an escalation. If State A wants to cause confusion by cutting off the communications of State B and the former has the cyber capability to either temporarily disrupt comms or use cyber to physically destroy

---

155 Siskind, Geoff "Hackable Podcast by McAfee," McAfee, February 2019, https://hackablepodcast.com/.

communications infrastructure, why risk the fallout of physical destruction when temporary disruption achieves the same purpose?

This is the primary reason that large scale attacks on physical infrastructure—while possible and may even occur from time to time—will remain much rarer than other forms of cyber operations and will likely only occur within a highly limited scope—such as in the Stuxnet and the attack seen in the Ukraine conflict. Conducting violent attacks that result in permanent damage to a state is—in most cases— counterproductive to the reason a state would be using a cyber attack in the first place.

The collateral damage risk is another reason a state would want to avoid conducting large scale, physically damaging attacks. Because of how interconnected networked systems are by nature, it is often difficult to estimate the amount of collateral damage done when a cyber attack is executed. This is less of an issue when the cyber operation only results in temporary disruption—if systems that are not the original target suffer temporarily, that may be an acceptable risk. However, if the attack is designed to cause permanent damage or even death, the risk of the attack spilling over to a system that is not the intended target may be too great for a state to risk. At that point, it would be more reasonable for a state to conduct the attack via precision physical weapons because the collateral damage is more controllable. If a political objective requires the use of violent action or death, it would be more effectively executed using conventional methods because—if an attack results in violence or death—escalation in retaliation may occur anyway, regardless of attack vector.

In conclusion, cyber operations are effective as a political tool in solving geopolitical challenges and goals where escalation to physical conflict is not desired. This desire for avoiding physical conflict helps provide a restraint to what type of cyber operations will be conducted. Just because a cyber attack "could" achieve a certain effect does not mean it "should" be used that way. The best use of cyber capabilities depends on the geopolitical goal trying to be achieved by its use. Both Russia and China have the technical capability to do physical, catastrophic harm through cyber attacks,[156] but that would defeat the purpose and many of the benefits of cyber tools over traditional hard power.

156 Coats, Daniel (Director of National Security), "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, (29 January, 2019).

CONCLUSION

With the return of nation-state rivalry, cyber operations provide a variety of options in influencing competitors when soft power actions are not enough or not desired. As networked connectivity further saturates every corner of the globe and every aspect of daily interactions, cyber attacks will become just as normal in the international sphere as economic negotiations, sanctions, and other everyday soft power moves. However, these gray zone cyber acts will deliberately be executed in such a manner as to avoid armed retaliation or lethality, thus limiting the scope and damage of cyber operations. Information warfare, influence operations, espionage, theft, and temporary infrastructure disruption are just a few of the new tools for states as revisionist powers look for new methods to gain objectives in the coming decades.

Contrary to many, networked technology does not make geography and state borders irrelevant. Rather, technological capabilities are bounded by geopolitics.[157] Geography, borders (such as waterways and mountain ranges), and natural resources still shape the strategic goals of a state and therefore shape how cyber is best used a tool. Despite all the unique benefits that cyber operations provide to a revisionist state and the regularity at which they will occur in the future, their geopolitical goals will define when and what type of cyber operations are the best tool to use.

---

157 Kaplan, Robert *The Revenge of Geography* (New York, New York: Random House, 2013).

BIBLIOGRAPHY

Bartz, Diane & Stubbs, Jack "U.S., Allies Slam China for Economic Espionage, Spies Indicted," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-usa/u-s-slams-china-for-corporate-cyber-espionage-indicts-two-spies idUSKCN1OJ1VN.

Barysevich, Andrei "Dissecting the Costs of Cybercriminal Operations," Recorded Future, November 2017, https://go.recordedfuture.com/hubfs/cyber-operations-cost-appendix.pdf.

Bettencourt, Jessica "The Olympic False Flag: Infamous OlympicDestroyer Malware Designed to Confuse Cybersecurity, Community," Kapersky Labs, March 2018, https://usa.kaspersky.com/about/press-releases/2018_the-olympic-false-flag.

Bing, Christopher "Exclusive: Clues in Marriott Hack Implicate China - Sources," Reuters, December 2018, https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D?mod=djem10point.

Blank, Stephen "Cyber War and Information War a la Russe" in *Understanding Cyber Conflict: 14 Analogies* (Washington DC: Georgetown University Press, 2017).

Blue, Violet "Hackonomics: Street Prices for Black Market Bugs," ZDNet, April 2014, https://www.zdnet.com/article/hackonomics-street-prices-for-black-market-bugs/.

Brown, Ian "Imagining a Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust," War on the Rocks, May 2018, https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust/.

Celso, Anthony "The 'Caliphate' in the Digital Age: The Islamic State's Challenge to the Global Liberal Order," *The International Journal of Interdisciplinary Global Studies*, Volume X, Issue X, (2015).

Coats, Daniel (Director of National Security) "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, (29 January, 2019).

Dinniss, Heather Harrison "The Regulation of Cyber Warfare Under the *Jus in Bello"* in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

Dubik, James, Lt Gen, (U.S. Army, Ret.) & Vincent, Nic "America's Global Competitions: The Gray Zone in Context," Institute for the Study of War, (February 2018).

Ferkoun, Maamar "Cloud Computing Helps Agriculture Industry Grow," IBM, January 2015, https://www.ibm.com/blogs/cloud-computing/2015/01/23/cloud-computing-helps-agriculture-industry-grow/.

Green, James "The Regulation of Cyber Warfare Under the *Jus ad Bellum"* in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

Greenberg, Andy "Hackers Remotely Kill a Jeep on the Highway—With Me In It," Wired, July 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Greenberg, Andy "Russian Hacker False Flags Work—Even After They're Exposed," Wired, February 2018, https://www.wired.com/story/russia-false-flag-hacks/.

Greenfield, Charlotte "New Zealand Intelligence Agency Joins Allies in Blaming Chinese Government for Hacking," Reuters, December 2018, https://www.reuters.com/article/us-china-cyber-newzealand/new-zealand-intelligence-agency-joins-allies-in-blaming-chinese-government-for-hacking-idUSKCN1OJ2M1.

Hodges, Duncan & Creese, Sadie "Understanding Cyber-Attacks," in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

Hutchins, Eric "The Cyber Kill Chain," Lockheed Martin, 2019, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

International Telecommunications Union, "ICT Facts and Figures 2017," ITU, 2017, https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

Jaitner, Margarita "Russian Information Warfare: Lessons From Ukraine," *NATO Coorperative Cyber Defense Center of Excellence*, (2015).

Jenkins, Tricia "What did the Russian Trolls Want During the 2016 Election: A Closer Look at the Internet Research Agency's Active Measures," War on the Rocks, May 2018, https://warontherocks.com/2018/05/what-did-russian-trolls-want-during-the-2016-election-a-closer-look-at-the-internet-research-agencys-active-measures/.

Kaplan, Robert *The Revenge of Geography* (New York, New York: Random House, 2013).

Kennedy, Patrick & Prat, Andrea "Where Do People Get Their News?" in 67th Economic Policy Panel Meeting, (Zurich, Switzerland: Swiss National Bank, April 2018).

Kofman, Michael "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," War on the Rocks, June 2018, https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/.

Lueth, Knud "State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating," IoT Analytics, August 2018, https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

Mello, Ulisses & Raghavan, Sriram "Bringing the power of Watson to farmers," IBM, September 2018, https://www.ibm.com/blogs/research/2018/09/smarter-farms-agriculture/.

Pihelgas, Mauno “Mitigating Risks Arising From False-Flag and No-Flag Cyber Attacks,” *NATO Coorperative Cyber Defense Center of Excellence*, (May 2015).

Rowe, Neil “The Attribution of Cyber Warfare,” in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security*,* 2016).

Sanger, David & Erlanger, Steven “Suspicion Falls on Russia as ‘Snake’ Cyberattacks Target Ukraine’s Government,” New York Times, March 2014, https:// www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html.

Schmidt, Eric & Cohen, Jared *The New Digital Age: Transforming Nations, Businesses, and our Lives* (New York, New York: Vintage Books, March 2014).

Scott, Laurence *The Four-Dimensional Human: Ways of Being in the Digital World* (London, England: Random House, 2015).

Segal, Adam *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York, New York: Public Affairs, February 2016).

Shearer, Elisa & Gottfried, Jeffrey “News Use Across Social Media Platforms 2017,” Pew Research Center, September 2017, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

Siskind, Geoff "Hackable Podcast by McAfee," McAfee, February 2019, https://hackablepodcast.com/.

Snegovaya, Maria "Putin's Information Warfare in Ukraine," *Institute for the Study of War*, (September 2015).

Statista, "E-commerce Share of Total Retail Sales in United States From 2013 to 2021," https://www.statista.com/statistics/379112/e-commerce-share-of-retail-sales-in-us/.

Steed, Danny "The Strategic Implications of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

Stiennon, Richard "A Short History of Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

Valeriano, Brandon & Maness, Ryan *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (New York, New York: Oxford University Press, 2015).

Whetham, David & Lucas, George Jr "The Relevance of the Just War Tradition to Cyber Warfare," in *Cyber Warfare: A Multidisciplinary Analysis (*New York, New York: Routledge Sudies in Conflict, Technology, and Security, 2016).

Wueest, Candid “Targeted Attacks Against the Energy Sector,” Symantec, (13 Jan 2014).

Yardley, Tim “SCADA: Issues, Vulnerabilities, and Future Directions,” Login Vol 33, no 6. (December 2008).