



Fordham University
DigitalResearch@Fordham

Senior Theses


International Studies

Spring 5-16-2020

Hacking Nation-State Relationships: Exploiting the Vulnerability of the Liberal International Order

Ray Marie Tischio

Follow this and additional works at: https://fordham.bepress.com/international_senior

 Part of the [International and Area Studies Commons](#)

Hacking Nation-State Relationships: Exploiting the Vulnerability of the Liberal International Order

Ray Marie Tischio

rtischio@fordham.edu

International Studies: Global Affairs Track
Fordham University Class of 2020

Thesis Advisor: Christopher Toulouse

toulouse@fordham.edu

Seminar Advisor: Dotan Leshem

dleshem@fordham.edu

ABSTRACT

This thesis explores the implications of nation-state cyberwarfare and cyber conflict in the context of geopolitics and international studies. The emergence of nation-state cyber conflict has increased in frequency and severity in the last decade. In order to investigate what renders cyberwarfare a new and unique challenge to specific geopolitical climates and international systems at large, research on state-level cyber conflict within bilateral relationships—all of which cyber activity is significantly prevalent—is presented in the following three case studies: US-China, US-Iran, and US-Russia. Findings of these three case studies are used in subsequent analysis to articulate the specific ways in which state cyber conflict differs from conventional state kinetic warfare. Finally, after characterizing cyber conflict and the new challenges it presents to geopolitics, these defining qualities are situated into the current debate surrounding the deterioration of the liberal international order. I conclude that nation-state cyberwarfare exploits the postwar interconnected transparency of liberalism, and fundamentally challenges the continuity of US hegemony and the liberal order.

Keywords: cyber conflict, cyberwarfare, espionage, liberal international order, national security, cybersecurity, cyberspace

ABBREVIATIONS

APT - Advanced Persistent Threat
CCP - Chinese Communist Party
CNI - Critical National Infrastructure
CSIS - Center for Strategic and International Studies
DDoS - Distributed Denial of Service
DHS - Department of Homeland Security (US)
DNC - Democratic National Committee
ECIR - Explorations in Cyber International Relations
FBI - Federal Bureau of Investigation (US)
FSB - Federal Security Service (Russia)
GRU - Main Intelligence Directorate (Russia)
HST - Hegemonic Stability Theory
ICS - Industrial Control Systems
ILSA - Iran-Libya Sanctions Act
IO - International Organization
IoT - Internet of Things
JCPOA - Joint Comprehensive Plan of Action
LIO - Liberal International Order
MSS - Ministry of State Security (China)
NATO - North American Treaty Organization
NCIX - National Counterintelligence Executive
NCSC - National Counterintelligence and Security Center
NSA - National Security Agency (US)
OPM - Office of Personnel Management
PLA - People's Liberation Army (China)
IRGC - Islamic Revolutionary Guard Corps (Iran)
USCC - United States Cyber Command (US)
SVR - Foreign Intelligence Service (Russia)

TABLE OF CONTENTS

| | |
|-------------------------------------------------------------------------|-----|
| Abstract | x |
| Abbreviations | xi |
| Table of Contents | xii |
| Introduction | 1 |
| Methodology | 2 |
| Literature Review | 4 |
| Case Studies | 8 |
| United States-China..... | 9 |
| United States-Iran..... | 15 |
| United States-Russia..... | 23 |
| Cyber Conflict: What Makes it Unique? Analysis | 30 |
| Cyberwarfare and the Liberal International Order: Analysis | 34 |
| Defining Liberal International Order | 35 |
| Cyber conflict as a challenge..... | 37 |
| Conclusion | 39 |
| Appendix | |
| Bibliography | |

Introduction

In a world governed by nation-states that is increasingly reliant on digital systems, it is no surprise that national security is correspondingly becoming synonymous with cybersecurity. Although the scope of cyber conflict is broad and continues to expand with the prominence of new technologies such as IoT devices, along with the rise of non-state actors such as cyber-criminal enterprises and hacktivist groups in their use of cyber methods to achieve deliberate goals, the scope of this thesis is focused solely on nation-state cyber conflict. In the last decade, the world has witnessed an increasing prevalence of nation-state cyber operations, and according to Evan Kohlmann, CIO at US-based business risk and threat intelligence firm Flashpoint (and also where I have been working as a software engineer intern since June), “the world is going to see more coordinated cyber operations from state-sponsored actors.”¹ The effectiveness of state-sponsored cyber operations in particular is due to their advanced capability and resources; often, these actors are referred to as APT groups, referencing the advanced persistent threat that they pose. Since only 2010, nation-state utilization of cyber approaches, methods and techniques have ensued unprecedented outcomes, ranging from physical destruction of nuclear facilities and intrusion into electrical power grids, to democratic election hacking and systematic theft of intellectual property at nearly every sector of society. Despite some warranted skepticism surrounding aggrandized fear of an imminent “cyber Pearl Harbor,” this unconventional type of conflict is undoubtedly impacting state relationships and broader political trends, and vice versa.

The sources in the literature review to follow are primarily derived from books, academic journals, news articles, and published reports. This thesis examines relevant scholarship and case studies of three nation-state bilateral relationships to synthesize the unique qualities of state

¹ Naushad K. Cherrayil, “State-sponsored actors to launch more coordinated cyber attacks,” *TechRadar*, October 9, 2019, <https://www.techradar.com/news/state-sponsored-actors-to-launch-more-coordinated-cyber-attacks>

cyber conflict and how they differ from state kinetic warfare, in order to more broadly discuss the role of cyber conflict in implicating and challenging the unipolar US-led power distribution and liberal international order.

Methodology

The exploration aim of this thesis is two-fold. Primarily, I will draw from case study findings to elucidate aspects and ways in which state cyber conflict differs from conventional modes of kinetic warfare, and add to aspects already defined in literature. Once these qualities that constitute cyber conflict are established, *how* these qualities interact with broader world systems will become a part of a larger attempt to situate implications of cyberwarfare within the current debate of the shifting LIO. Nation-state cyber conflict and operations in this thesis is *not* limited to only cyber “attacks,” but also includes cyber espionage and information warfare. The exact definition of cyberwarfare tends to vary depending upon the lens through which it is analyzed, and sometimes does not include espionage or disinformation tactics; however, for the purpose of contextualizing cyber strategy within nation-state relationships, these prominent areas of cyber operations will be included in case study analysis and discussion.

Particularly, I will explore how state governments utilize cyber strategies to act on foreign policy objectives, assert their own state power or alter existing power dynamics, and integrate them into approaches to bilateral relationships. Individually, each of the three case studies will scrutinize approaches, methods, and consequences of cyberwarfare and cyber conflict in the following significant state bilateral relationships, all of which cyber conflict has played a considerable role: the US and China, the US and Iran, the US and Russia. These four nation-states were chosen particularly due to their advanced use and demonstration of cyber capability and record of willingness to utilize cyberattack methods in order to act on a state

objective or attain a state goal. In addition to their relevance, these studies are *necessary* in order to understand the nuanced differences between how these cyber powers approach this novel type of warfare, what state objectives are actioned on by using cyber methods, and what broader consequences, if any, cyber conflict presents to each unique bilateral relationship. Each of the three chosen relationships involve the United States, and this is intentional; because one of the ultimate goals of this thesis is to explore the geopolitical power implications of state cyber conflict within the context of the western-led liberal order, the implications for continuity of US power and hegemonic status will be of particular interest. There is no existing literature that focuses specifically on the propensity of cyber conflict to challenge the LIO. Before attempting to address this in later discussion, the following section will review relevant literature by introducing important background of nation-state cyberwarfare, and will briefly substantiate the importance of exploring this topic in the current context of international relations.

This research was designed based on my interest in the intersection of the traditionally separate realms of technologically-dominated fields of computer science and cybersecurity, and the field of international studies. Cyberwarfare and cyber conflict, especially at the nation-state level, is a topic which ought to be examined and considered with an interdisciplinary approach as it necessitates both technical and geopolitical knowledge. Given my background in computer science and international studies, I aim to contribute not only to the dialogue on the topic, but also to the synergy of both fields within scholarship, as they increasingly become more relevant to one another. I welcome the use of technical sources, and plan to incorporate useful technical information into my research and analysis.

Literature Review

The introduction of cyber conflict into the scope of international relations is relatively recent. Most literature on the subject has been written in the last decade, and in an increasing frequency within the last five years. Often, literature on the subject is concerned with urging attention to the realm of cyberspace and its implications. Experts Nazli Choucri and David Clark go beyond this; as they comprehensively place the cyber domain within the setting of international relations, they introduce the cyber-IR model, in order to develop a “cyber-inclusive view of international relations... to anticipate and respond to cyber threats, impacts on power politics, and challenges to national security and international stability,” and contextualize the “co-evolution” of both cyberspace and international relations.² As cyberspace has been established as the fifth domain following land, sea, air and space,³ and as national security is increasingly synonymous with cybersecurity, it is growingly obvious that there is critical bridging to be done between the fields of technology and foreign policy. Choucri and Clark’s work within the *Explorations in Cyber-IR* Harvard-MIT project has made great strides to integrate these already inextricably linked spheres of knowledge, while bringing expertise from political science and computer science, respectively.

It is no surprise that cybersecurity is becoming more important at all levels of society, as individuals and institutions rely more and more on digitized infrastructure. The World Economic Forum’s Global Risks Report 2019, published at the beginning of this year, urges attention to

² Choucri, Nazli and David D. Clark. “International Relations in the Cyber Age: The Co-Evolution Dilemma.” Cambridge: *MIT Press*, 2019. <https://ieeexplore.ieee.org/servlet/opac?bknumber=8671655>

³ “War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?” *The Economist*, July 1 2010. <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>

cyberspace and its potential for global impact. Massive data fraud and theft was ranked as the fourth major global risk, alongside cyberattacks, closely ranked at fifth. As seen in Appendix A, cyber-risks are situated in the high-impact and high-likelihood quadrant of the WEF Global Risks Landscape graph—second only to environmental risks. As denoted in their report, these figures signify the “instabilities [which] are being caused by the deepening integration of digital technologies into every aspect of life.”⁴ With more specificity, the Worldwide Threat Assessment, published by US intelligence and director of national intelligence at the time Daniel Coats, expands further upon these aforementioned threats. The 2018 report mentions the increased prevalence and availability of ransomware and malware attacks, and raises concerns about the “increasingly damaging effects of cyber operations and the apparent acceptance by adversaries of collateral damage.” Honing in on nation-state conflict, “states are using cyber operations as a low-cost tool of statecraft,” using them “to achieve strategic objectives unless they face clear repercussions.” A year later, an updated U.S. threat assessment report was published for 2019. It more fervently maintains that United States’ foreign adversaries will “increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage.” On the ground, these mentioned cyber capabilities translate into “steal[ing] information, influenc[ing] citizens, or disrupt[ing] critical infrastructure.”⁵ A report on nation-state motives behind today’s advanced cyberattacks, published by cybersecurity company FireEye acknowledges this range of nation-state cyber operations, titling it a “shadowy battlefield” in which governments clash and co-exist “in a new,

⁴ “The Global Risks Report 2019,” *World Economic Forum*, January 15, 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

⁵ Daniel R. Coats, “Worldwide Threat Assessment of the US Intelligence Community,” *Office of the Director of National Intelligence*, January 29, 2019. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>

mostly invisible theater of operations.”⁶ This report, like several others, advocates that cyberattacks are not arbitrary, one-off, meaningless acts of state aggression.⁷ Rather it argues that cyberattacks have “distinctive characteristics, which include everything from motivation to target to type of attack,” and that they are “not an end in [themselves].”⁸

Senior fellow at the George Washington University Center for Cyber and Homeland Security, Isaac Porche, comments on the prevalence of these types of cyber operations, claiming “nation-states and their proxies are spying and attacking in cyberspace across national borders with regularity.”⁹ Porche claims nation-state cyber-wars are not only a thing of the future, but of the present. Because of the severe lack of international norms and agreement concerning cyberspace, targeted cyber operations never meet the criteria of an act of war or aggression; however, if there were norms in place, perhaps some of these advanced and impactful attacks would no longer “fall into a gray area below the threshold of total war.”¹⁰ This gap in international frameworks is an exploitable uncertainty, according to Porche, and one that is worth attention, especially in light of the threat posed to critical infrastructure.¹¹ International and domestic frameworks that apply to kinetic warfare are outdated and irrelevant when acts of aggression from the cyber domain come into play; long-existing theories cannot be readily imported into handling nation-state cyber operations. At the very minimum, our institutions and norms must be applicable to this undeniably emerging pattern of warfare.

⁶ Kenneth Geers et al. “WORLD WAR C: Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks,” *FireEye*, (2014): 3. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf>

⁷ Mike Walls, “Nation-States: Why They Hack,” *EdgeWave*. (April, 2015): 1-12. http://www.edgewave.com/wp-content/uploads/2015/04/EdgeWave_NationStates_WhyTheyHack.pdf

⁸ Geers, 3.

⁹ Isaac Porche, “Getting Ready to Fight the Next (Cyber) War,” *RAND Corporation*, March 3, 2018, <https://www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html>

¹⁰ Isaac Porche III, “Fighting and Winning the Undeclared Cyber War,” *RAND Corporation*, June 24, 2019, <https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html>

¹¹ Porche, “Fighting and Winning the Undeclared Cyber War.”

Vulnerabilities, especially those found within critical infrastructure, intelligence agencies, and institutional systems, present cause for concern; over the last decade, nation-states, including the United States have witnessed sophisticated attacks and exploits. Some of these significant attacks will be discussed later in the three nation-state bilateral relationship case studies. Increased severity and increased frequency of cyberattacks warrant further focused exploration on this topic.

Rolling out new IoT devices, software, and expanding the amount of people who access mobile and internet devices regularly only increases the potential for new system vulnerabilities and their exploits by malicious actors. In addition, the speed at which this domain changes surpasses the realistic amount of time for countries and international organizational bodies to negotiate and legislate.¹² From a chart included in the 2018 Worldwide Threat Assessment Report published by US intelligence, it is evident that since 2007, there has been a significant jump in the total countries with cyberattack capability (See Appendix B). It is reasonable then to place importance on up-to-date data for both the technical exploits and the geopolitical affairs relevant to nation-state cyber strategy, especially due to its changing nature. In his book *War in Cyberspace*, former government official and counterterrorism expert Richard Clarke asserts that “cyber war is a wholly new form of combat, the implications of which we do not yet fully understand.”¹³ He comments further on the inherent nature of cyberwarfare which renders it different than 20th century warfare, and which will be the subject of discussion following the three case studies.

¹² Tarah Wheeler, “In Cyberwar, There are No Rules,” *Foreign Policy Magazine*, September 12, 2018, <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/>

¹³ Richard Clarke, “War From Cyberspace,” *Center for the National Interest*, December 22, 2009, <https://nationalinterest.org/article/war-from-cyberspace-3278>

Case Studies

Each of the three case studies will begin by contextualizing recent and current background of the bilateral relationship, including points of conflict or tension. State cyber activity will follow the background section, and will be organized by major themes or trends; the thematic breakdown of each bilateral relationship is not intended to simplify or overly generalize the cyber conflict that exists or has existed between any given two states, but rather is meant to help organize sporadic incidents from the last decade and frame them in a relevant geopolitical context. Based on findings from this section of each study, I will lastly discuss broader objectives of what the particular nation-state utilizes cyber activity to achieve. In the field of cybersecurity, the *cyber kill chain* is a common framework used to identify, trace, assess and understand the stages of a cyberattack (See Appendix C).¹⁴ The final step of this cyber kill chain is *Actions on Objectives*, which serves to pinpoint goals and motivations behind a given cyberattack, which “vary greatly depending on the threat actor,” ranging from “political, financial, or military gain.”¹⁵ The state cyber activity section of each case study can be thought of as the ‘actions’ component, while the last section speaks to the ‘objectives’ and motivations behind the state’s cyber operations at large. The goal is to articulate *what* objectives state actors acted on through cyber operations, and *how* the state actors used cyber operations to act on these objectives. The Diamond Model of Intrusion Analysis is another technical approach to understanding cyberattacks, and it is worth noting the emphasis this model gives to understanding the social-political relationship and degree of persistence between adversary and

¹⁴ “The Cyber Kill Chain,” *Lockheed Martin*, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

¹⁵ Spitzner, Lance. “Applying Security Awareness to the Cyber Kill Chain,” *SANS Security Awareness*. May 31, 2019. <https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain>.

victim (See Appendix D).¹⁶ The case studies within this thesis have aims similar to these two technical models; however, rather than focusing on a particular incident, general trends of state cyber operation and activity will be of focus.

United States and China. Since the emergence of liberal international institutions during the postwar era, US and Chinese relations have continued to shift. At the dawn of the new century, US was paving the way for Chinese integration into liberal institutions such as the WTO. Prior, China had been on the outside of the liberal emergence that the US was leading; however normal trade relations between the two were established by 2000, and by 2006, China was the US' second-biggest trade partner. Global liberal integration continued, and China was increasingly recognized as an emerging power, becoming the world's second largest economy. China witnessed rapid change and benefited from the liberal institutions and integration, although it is not a democratic state.¹⁷ However, the rest of the 21st century US-Chinese relations have been characterized by conflict involving trade disputes and deficits. While continuing to prioritize their bilateral and economic relationship, during the Obama administration, cyberespionage became a topic of disagreement between the two leaders. As they agreed on steps towards climate change accords and concerns for denuclearization, the discussion of cyber activity served as a point of contention. In months prior, the US had accused Chinese corporations of state-sponsored cyber espionage, including theft of US military and economic secrets; this was met by only Chinese denial. The US warned that Chinese hacking and cyberespionage threatened the bilateral relationship both sides had been working toward. President Obama suggested that if this

¹⁶ Sergio Caltagirone, Christopher Betz, and Andrew Pendergast. "The Diamond Model of Intrusion Analysis." *Center for Cyber Threat Intelligence and Threat Research*. July 5, 2013. <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

¹⁷ "U.S. Relations with China." *Council on Foreign Relations*. <https://www.cfr.org/timeline/us-relations-china>

cyber activity continued, it would give rise to a “difficult problem in the economic relationship” as well.¹⁸

Some of this economic conflict has occurred jointly with increasing cyber activity (specifically, economic espionage and hacking), which both states claimed they were a victim of. During the Trump administration, this trade war has only intensified, and some initial tariffs were placed in response to cyber activity.¹⁹ The preceding bilateral relations between the two nation-states has underlined the way in which cyber operations continue to play a role in this relationship.

Prior to the Sunnylands Summit in 2013, the US established a branch of the military dedicated to cyber affairs (USCC) and additionally publicly declared “cyberspace as a new domain of warfare.”²⁰ According to expert Amy Chang, author of *Warring State: China’s Cybersecurity Strategy*, these two US actions had significant implications for how China perceived American motives at the time; Chinese media interpreted this as a threatening step towards a new destabilizing ‘cyber arms race,’ much like a cyber-version of the Cold War. This prompted some sentiment for China to “race in response, to ensure [they do] not fall behind.”²¹

The US would again (unintentionally) threaten the Chinese perception of their motives and intentions; in 2013, whistleblower Edward Snowden leaked confidential NSA strategy information which included a covert surveillance operation that amassed global communication data (the project known as PRISM). Other findings included NSA infiltration and exploitation of

¹⁸ Jackie Calmes and Steven Lee Myers, “U.S. and China Move Closer on North Korea, but Not on Cyberespionage,” *The New York Times*, June 8, 2013. <https://www.nytimes.com/2013/06/09/world/asia/obama-and-xi-try-building-a-new-model-for-china-us-ties.html>.

¹⁹ “U.S. Relations with China,” *Council on Foreign Relations*.

²⁰ Ibid.

²¹ Amy Chang, “Warring State: China’s Cybersecurity Strategy,” *Center for a New American Security*, (December 2014): 27 <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Warring%20State%20-%20China%27s%20cybersecurity%20strategy.pdf>

top-level Chinese military officials' computers. Ultimately, this leak proved the NSA's cyber espionage efforts were directed towards other nation-states, including China. According to Chang, these disclosures "reversed momentum towards what could have been a breakthrough in U.S.-China cyber relations"²² as witnessed during the Sunnylands summit. China used the Snowden leaks to point out US hypocrisy and "[show] once again that China falls victim to cyberattacks" when faced with cyber espionage accusations from the US, instead of attempting to cooperate towards a bilateral agreement.²³ Since Chinese leader Xi Jinping came to power, he has emphasized network security and informatization as two major components of the Chinese government's national security agenda. Tensions and developments in cyberspace have caused "negative externalities" on U.S.-China relations, and are crucial in defining broader trends of state cyber conflict approach.²⁴ This next section of the case study is intended to survey prominent aspects of state cyber conflict and state cyber operations specifically within the US-China bilateral relationship.

State-sponsored cyber activity. Within the last decade, China as a leading cyber power has been heavily associated with economic espionage, and this is not unwarranted; China's state cyber operations are predominantly focused on economic espionage efforts. The US National Counterintelligence Executive office (NCIX) has described Chinese state cyber actors as "the world's most active and persistent perpetrators of economic espionage."²⁵ Although cyber espionage is not always included in the definition of *cyberwarfare*, China's extensive cyber espionage campaign has implicated and continues to threaten the security of the US government

²² Chang, 38.

²³ Ibid.

²⁴ Chang, 12.

²⁵ "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World." *White House Office of Trade and Manufacturing Policy*. (June 2018): 1-36.

as well as many other states, industries and institutions. The Council on Foreign Relations database of cyber operations incidents now classifies 123 of 128 Chinese cyber operations as being of espionage intent.²⁶ The US FBI defines economic espionage as “foreign power-sponsored or coordinated intelligence activity... designed to unlawfully or clandestinely influence... or obtain” proprietary information in areas such as technology, finance and government policy.²⁷ This includes economic intelligence, confidential trade information, and intellectual property. Further, the resulting ‘theft’ from economic espionage benefits the perpetrating state, while causing “significant economic losses” to the victim (often by undermining costs for research and development).²⁸ It is worth noting that the clandestine nature of espionage, especially through cyber means (as is the focus here), renders comprehensive and complete measures of Chinese efforts and/or impacts much more difficult. Knowledge of such efforts is limited not only to what is publicly released, but is also limited to what efforts have been recognized *and* attributed. The major public beginnings of US-Chinese cyber conflict begins also with the first ever instance of state charges against an alleged state cyber actor.²⁹ Although, it is important to keep in mind that cyber espionage had already been occurring less publically for some years—CSIS dates their *Significant Cyber Events* timeline back to 2006, for example listing China’s hacking the Department of State’s networks and “download[ing] terabytes of information.”³⁰ In 2014, the FBI indicted five Chinese hackers, all of whom were

²⁶ The Council on Foreign Relations database is available for download from Council on Foreign Relations, undated. <https://www.cfr.org/interactive/cyber-operations#CyberOperations>

²⁷ “What is Economic Espionage?” *Federal Bureau of Investigation*, (2019) <https://www.fbi.gov/about/faqs/what-is-economic-espionage>

²⁸ Daniel Liberto, “Economic Espionage,” *Investopedia*, (2019) <https://www.investopedia.com/terms/e/economic-espionage.asp>

²⁹ Adam Segal, *The Hacked World Order* (New York: PublicAffairs 2016), 137.

³⁰ “Significant Cyber Incidents,” *Center for Strategic and International Studies*, November, 2019. <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

officers in Unit 61398 of China's PLA.³¹ The FBI's charges included stealing confidential internal strategy data and other manufacturing and technology business intellectual property from U.S. subsidiaries such as U.S. Steel Corporation and other private companies.

Based on their research and observation, security firm Mandiant concluded that one of the most prominent, persistent, and "prolific cyber espionage groups" is confidently believed to be the PLA's Third Department (Unit 61398).³² China is known in the cybersecurity world for its focus on espionage with an extensive range of targets, from commercial to political; for example, during the 2008 US presidential election, the campaigns of both Obama and McCain were victims of a massive cyber espionage operation led by the Chinese government, which intruded and penetrated these networks to export internal data.³³ In 2015, 70 percent of America's corporate intellectual property theft [was] believed to originate from China.³⁴ More recently, the 'advanced persistent threat' of China has had implications in its recent trade war with the US; fear of this threat has spurred heavy tariffs as well as a ban on giant telecommunications firms' products (Huawei and ZTE), as the US is distrusting of these products due to their close ties with the Chinese government, and government-sponsored espionage. Some of the surrounding fears include the possibility that the government encourages the "install[ation] [of] backdoors into its products which would allow China to spy on network traffic, potentially on a global scale."³⁵

The US fears Huawei's success in developing global 5G networks "will give Beijing an

³¹"U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage," *U.S. Department of Justice*, July 14, 2015.

³² "APT1: Exposing One of China's Cyber Espionage Units," *Mandiant*. Accessed November 12, 2019. <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

³³ Michael Isikoff, "Chinese hacked Obama, McCain campaigns, took internal documents, officials say." *NBC News*. (2013) <http://www.nbcnews.com/id/52133016/t/chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say/#.Xfcu5ufYrBJ>

³⁴ Ian Bremmer, "These 5 Facts Explain the Threat of Cyberwarfare.", *TIME Magazine*. June 19, 2015. <https://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/>

³⁵ Matt Burgess, "Is China Really Using Huawei to Hack the World's Communications?" *WIRED Magazine*, January 25, 2019. <https://www.wired.co.uk/article/huawei-5g-uk-security>

unprecedented opportunity to attack critical infrastructure and compromise intelligence sharing...” potentially entailing “cyberattacks on public utilities, communication networks and key financial centers.”³⁶

Units 61398 and 61486 of China’s PLA are two out of many Chinese cyber espionage groups targeting political and military intelligence in their efforts, as well as generally any “info to bolster China's economic competitiveness.”³⁷ Over two dozen US Department of Defense weapons programs have been hacked and had data compromised. The major Office of Personnel Management (OPM) breach had been occurring since 2013, but was not fully recognized or released until 2015, and not officially attributed to China until 2018. The Chinese state group behind the attack compromised 22 million records of personal information, ranging from security data on military and intelligence personnel, to fingerprint data of almost six million people. This severely threatened the national security of the US; the breached confidential data would enable the Chinese government to identify US covert spies working abroad. China’s Ministry of State Security (MSS), another governmental agency responsible for cyber operations, “reportedly combined medical data stolen from Anthem insurance, travel records from United Airlines and OPM security files to create a more complete picture of US officials,” worth noting to highlight the strategic breadth and ability of these state actors. Former counsel at NSA, Joel Brenner, termed the OPM incident “a significant blow” to American intelligence.³⁸

In addition to government intelligence and intellectual property, Chinese state-sponsored actors have also been linked to theft of confidential US military and defense data. This has been

³⁶ Bryan-Low Cassell et al., “Special Report - Hobbling Huawei: Inside the U.S. War on China’s Tech Giant,” *Reuters*, May 21, 2019. <https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-us-war-on-chinas-tech-giant-idUSKCN1SR1EU>

³⁷ David. E. Sanger et al., “Chinese Army Unit is Seen as Tied to Hacking Against U.S.” *The New York Times*, February 18, 2013. <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>

³⁸ Segal, 140.

exemplified by significantly similar-looking stealth fighter jets developed recently, and have even been referred to as “knockoffs” of US-designed jets.³⁹

China’s state-sponsored cyber espionage and operations described above reflect efforts to act on unique state objectives. This includes China’s desire to reduce the ‘technology gap’ between it and the US; their targeting of research and innovation data corresponds to this objective, as “China doesn’t want to... run the risk of remaining second-tier manufacturing specialists that lack innovation needed to become global technology leaders” while relying on advanced technologies from other states.⁴⁰ Additionally, China’s state objectives include upholding and maintaining the Chinese Communist Party (CCP). Military development is a key way in which China sees this as being done, as their cyber operations have reflected the goal of military modernization, “while simultaneously preparing for the possibility of militarized cyber conflict in the future.”⁴¹

United States and Iran. Understanding the “extremely sensitive”⁴² US-Iran bilateral relationship contextualizes the objectives acted on by both states in their state-sponsored cyber activity. Dating back to the end of the Iranian Revolution in 1979 and the Iran hostage crisis, diplomatic tension has underscored their relations, as the US has continued to maintain a physical military presence in the region. Economic relations between the two have similarly been strained as a result of many factors; the Clinton administration imposed a complete embargo on Iran in 1995, and in 1996 established the Iran and Libya Sanctions Act of 1996 (ILSA), placing sanctions on

³⁹ Jeff Daniels, “Chinese theft of sensitive US military technology is still a ‘huge problem,’ says defense analyst,” *CNBC News*, November 8, 2017, <https://www.cbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html>

⁴⁰ Segal, 153.

⁴¹ Chang, 7.

⁴² Walls, “Nation-States, Why They Hack,” 6.

non-American companies investing in the Iranian oil and natural gas industries.⁴³ The US-Iran relationship in the early 2000s was newly fraught with fears of nuclear build-up and aggression as Iran began their development of nuclear facilities, and denied US accusations of a secretive nuclear weapons program. Sanctions on Iran by the US, EU, and the UN continued into the start of the new century.⁴⁴ As will be discussed in the following section, it is this tension that defined the relationship until cyber operations became an additional point of agitation. The discovery of the Stuxnet malware and Operation Olympic Games in 2010 would prove to be a turning point in Iranian state approach to cyber conflict. It was not until 2015 that diplomatic efforts from Iran and the P5+1 finally reached an agreement on the long-term Iran Nuclear Deal (formally known as the Joint Comprehensive Plan of Action, JCPOA), under which Iran agreed to limit nuclear development activity and allow UN inspection in exchange for the lifting of economic sanctions. However more recently, President Donald Trump withdrew the US from this deal and reinstated decades-old sanctions, which only worsened relations between the US and Iran.⁴⁵

State-sponsored cyber activity. In an attempt to define themes of Iranian state-sponsored cyber operations in relation to (probable) motives, several sources and scholars have articulated *retaliation* as a necessary factor to understanding Iranian hacking. Hacking activity has been originating from Iran since the early 2000's, largely in the form of "patriotic hacking"—less sophisticated operations such as website defacements, or domestically focused activity, not initiated by a legitimate branch of the Iranian military.⁴⁶ However, in 2010, Iran became known as one of the world's first public targets and victims of serious state-sponsored cyberwarfare

⁴³ Lionel Beehner, "Timeline: U.S.-Iran Contacts," *Council on Foreign Relations*, March 9, 2007. <https://www.cfr.org/background/timeline-us-iran-contacts>

⁴⁴ "US-Iran relations: A brief history," *BBC News*, June 21, 2019 <https://www.bbc.com/news/world-middle-east-24316661>

⁴⁵ Ibid.

⁴⁶ Hodgson et al., *Fighting Shadows in the Dark, Understanding and Countering Coercion in Cyberspace*, (Santa Monica, CA: RAND Corporation, 2019): 23.

upon the discovery of the Stuxnet virus. The Stuxnet virus was a global turning point for cyberwarfare and state cyber operations, with implications that extend far outside of the US-Iran relationship; it is considered by many to be the first direct example of cyberwarfare and the first cyberwarfare weapon,⁴⁷ and was in fact the “first cyberattack ever designed to directly damage physical equipment.”⁴⁸ This malware was designed to physically destroy the centrifuges of Iran’s nuclear facilities, and was attributed to an US-Israeli joint operation. It was likely designed in 2005-2007, and was persistent until its discovery in 2010; by this time, it had destroyed over a thousand centrifuges of Iran’s Natanz nuclear facility.⁴⁹ This directed operation precipitated a fundamental shift in how Iran would approach cyber operations at the state level from then on, as well as what their motives behind cyber operations would be. Retaliation in the form of advancing cyber activity was quickly seen, as soon as 2011.⁵⁰ Iran invested in a focused effort to invest and develop cyber capabilities,⁵¹ as was demonstrated by their establishment of their Supreme Cyberspace Council.⁵²

Following the 2010 detection of the consequential Stuxnet worm, a string of advanced and arguably retaliatory cyberattacks originated from Iran. The first Iranian-attributed cyber espionage campaign (Madi, targeting the US and Iran’s regional adversaries), the first delivery of the Shamoon malware (targeting Saudi Aramco, one of the world’s largest oil companies and Qatari RasGas corporation⁵³), and the first series of DDoS attacks on some of the largest US banks (Operation Ababil) all only within the second half of 2012.⁵⁴ These cyberattacks served as

⁴⁷Langner, R., “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE Security & Privacy* 9 (2011): 49-51.

⁴⁸Andy Greenberg, “The WIRED Guide to Cyberwar.” *WIRED Magazine*, (2019) <https://www.wired.com/story/cyberwar-guide/>

⁴⁹Jim Frankle, “Researchers say Stuxnet was deployed against Iran in 2007,” *Reuters*. February 26, 2013.

⁵⁰“Cylance Operation Cleaver Report,” *Cylance*, December 23, 2016.

⁵¹Walls, “Nation-States: Why They Hack,” 7.

⁵²Hodgson et al., 23.

⁵³“Compromise of Saudi Aramco and RasGas,” *Council on Foreign Relations*, Accessed November 12, 2019.

⁵⁴“Iran’s Cyber Threat: Timeline,” *Carnegie Endowment for International Peace*, January 4, 2018.

the first glimpse into Iran's advanced, bold, and rapidly-developed cyber capabilities, as well as their intention for their cyber operations.

Aside from geostrategic retaliation, Iran has also demonstrated their influence of retaliation as motive for direct industry-targeted cyberattacks. In 2014, Iranian state-sponsored hackers launched a destructive cyberattack on Sands Las Vegas Casino Corporation; data was stolen and destroyed, computers were wiped, and the company was frozen by this malware infection.⁵⁵ The *retaliation* aspect of this operation is evident, as the casino's owner Sheldon Adelson is a vocal pro-Israel who had publicly suggested the US drop nuclear bombs on Iran.⁵⁶ The nation-state actors behind the attack made their retaliation known, leaving behind a message on the infiltrated computers which denounced "encouraging the use of Weapons of Mass Destruction" as a crime.⁵⁷ Iranian state cyber operations have been quite regionally focused in the past, and targeted at countries nearby such as Saudi Arabia and Israel, however Iran increasingly targets US industry and technologies as well, threatening US national security. Like other state actors, Iran targets specific commercial industries in order to develop and bolster those of its own. At large, previously targeted industries have included 1) military and defense-related; 2) natural resources and energy; 3) telecommunications; 4) infrastructure.⁵⁸

Certain Iranian state-sponsored cyber-active groups (such as Rocket Kitten) often target US defense firms in their cyber operations, and are likely motivated by an agenda to modernize their military and improve and advance their missile and space programs using stolen

⁵⁵ Jose Pagliery, "Iran Hacked an American Casino, U.S. Says," *CNN Business*, February 27, 2015. <https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html>

⁵⁶ Ibid.

⁵⁷ Andy Greenberg, "The Iran Nuclear Deal's Unraveling Raises Fears of Cyberattacks," *WIRED Magazine*, May 5, 2018. <https://www.wired.com/story/iran-nuclear-deal-cyberattacks/>

⁵⁸ Ed Parsons and George Michael, "Understanding the Cyber Threat from Iran," *F-Secure Cyber Security*, Accessed November 10, 2019. <https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran>

“proprietary and sensitive US military technology.”⁵⁹ Other groups (such as APT33) have used advanced cyber techniques to target US aerospace and civil aviation firms,⁶⁰ as well as energy sector companies, aligning with Iran’s agenda to improve one of its largest industries and exports — petrochemical production and technology.⁶¹ Operation Newscaster was a notable example of an elaborate and long-term cyber espionage operation, targeting intelligence and public policy information from military and political figures of Western states (including the US) as well as other regional adversaries from 2011-2014.⁶² Espionage efforts have also been aimed at stealing intellectual property and proprietary data from American corporations such as HBO, as well as US financial institutions and information technology companies.⁶³ Iran responded by launching massive DDoS attacks against the US financial sector in 2012, after the US launched sanctions against Iran and only two years after Stuxnet was exposed.⁶⁴ However, the US and Israel also jointly took part in developing sophisticated cyber espionage, sabotage, and “cyber-collection” malware (Flame and Duqu) aimed at hindering Iranian nuclear development and conducting reconnaissance. These persistent-engaging attacks were discovered soon after Stuxnet.⁶⁵ Iran has additionally posed a risk to CNI in the past. In 2015, an Iranian cyberattack caused a complete power outage of the electrical grids in over half of Turkey’s provinces; from “computers, airports, traffic lights, hospitals, lights, elevators, refrigeration, water and sewage, everything

⁵⁹“Foreign Economic Espionage in Cyberspace,” *National Counterintelligence and Security Center*, (July 2018): 9. <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>

⁶⁰ Ibid.

⁶¹ Ibid.

⁶²Cheryl K. Chumley, “Iranian hackers sucker punch U.S. defense officials with creative social-media scam,” *The Washington Times*, May 29, 2014.

⁶³ “Foreign Economic Espionage in Cyberspace,” 10.

⁶⁴ Joe Uchill, “Iran’s History of Hacking and Being Hacked,” *Axios*, June 27, 2019. <https://www.axios.com/irans-history-of-hacking-and-being-hacked-ab1a9e96-63f1-4974-b75c-b72adc03dc51.html>

⁶⁵ Ellen Nakashima, Greg Miller and Julie Tate, “U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say,” *The Washington Post*, June 19, 2012.

simply stopped” for over 12 hours.⁶⁶ Although not a crucial element of US-Iranian bilateral relations, many experts interpreted this destructive attack as a “flex” of Iranian ability to disrupt CNI.⁶⁷ Not long before this, security firm Cylance published a report detailing Iran’s Operation Cleaver, which had at the time recently been detected as penetrating, attacking, “establishing persistence in, and extracting highly sensitive materials” of critical infrastructure targets of several nation-states, and mainly of the United States.⁶⁸

In addition, foreign academic institutions and universities are a frequent target. In 2018 it was found that Iran state-sponsored groups executed cyberattacks on 176 universities across 21 foreign countries; in the US alone, it was alleged in a 2018 indictment of nine Iranian nationals that 31 terabytes of documents and data had been stolen from over 140 universities,⁶⁹ as well as 30 companies and 5 government agencies.⁷⁰ Similarly to motivations underlying economic espionage, Iran’s targeting of academic intellectual property and unpublished research is derived from their objective of advancing their defense capabilities, development of nuclear power, and monitoring expatriates.⁷¹ This ongoing espionage campaign was led by Iran’s Islamic Revolutionary Guard Corps (IRGC)—a branch of their state armed forces—and was motivated by desired access to data, to ultimately benefit the Iranian government and peripheral state institutions.⁷²

According to the National Counterintelligence and Security Center’s (NCSC) 2018 publication on foreign economic espionage in cyberspace, Iran is predicted to continue

⁶⁶ Michah Halpern, “Iran Flexes Its Power by Transporting Turkey to the Stone Age,” *The Observer*. April 22, 2015,

⁶⁷ Ibid.

⁶⁸ “Cylance Operation Cleaver Report,” *Cylance*.

⁶⁹ “Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps,” *U.S. Department of Justice*, March 23, 2018.

⁷⁰ Catalin Cimpanu, “Iranian Hackers Charged in March Are Still Actively Phishing Universities,” *BleepingComputer*, (2018).

⁷¹ Ed Parsons and George Michael, “Understanding the Cyber Threat from Iran.”

⁷² “Foreign Economic Espionage in Cyberspace,” 10.

penetrating US and allied network infrastructure for espionage efforts as well as to “position itself for future cyberattacks.”⁷³ As Iran’s economy is significantly reliant on the oil industry and petroleum revenue, its longevity “will depend on growth in non-oil industries” and efforts of economic-diversification; a primary motive for cyber espionage efforts across industries. Similarly, cyber espionage targeting industry and academic institutions are motivated by attempts to lessen the gap in science, technology and research between Iran and Western states.⁷⁴

Aggression within the US-Iranian bilateral relationship has served as a “symbol of Western meddling in the region” from Iran’s frame of reference. In addition to economic objectives, Security operations and analysis expert Mike Walls posits the Iranian perspective as “also impacted by theology,” as it serves as an additional motivation behind Iranian cyber operations.⁷⁵ In a RAND Corporation 2019 publication on cyberspace coercion, the authors suggest that “Iran’s efforts suggest an orchestrated attempt to challenge its regional adversaries and gain a more prominent place as a regional power.”⁷⁶ Objectives of asserting regional dominance as well as religious dominance are interwoven. Expanding their sphere of influence in the Middle East would require Iran to challenge both the “military and economic influence of Western countries [maintaining] a presence in the region” as well as “destabilize those Sunni Islamic governments which are historically allied with” or supported economically or militarily by the West.⁷⁷ These Western alliances with Sunni states, including Saudi Arabia, Kuwait, Jordan and Egypt, continue to create regional tension as Iran exerts its dominance. The regional religious distinction between Iran’s Shi’a state and the more popular Sunni sect of Islam is

⁷³ Hodgson et. al., 26.

⁷⁴ “Foreign Economic Espionage in Cyberspace,” 10.

⁷⁵ Walls, “Nation-States: Why They Hack,” 6.

⁷⁶ Hodgson et. al., 27.

⁷⁷ Walls, “Why Iran Hacks.”

significant because hostility between the two is a “root cause of the persistent tension in the region.”⁷⁸ In *Why Iran Hacks* of his multiple-part series, Walls explains “as Iran continues to leverage the threat of nuclear weapons in the kinetic world, it is actively converting threat to action in the cyber domain to achieve its regional objectives.”⁷⁹

In addition to utilizing cyber means to act on regional objectives, Iran’s cyber activities and operations coincide with broader geostrategic progressions. A RAND Corporation publication from 2019 acknowledges the timing of turning points in Iran’s cyber activity in comparison with that of diplomatic agreement or other significant events. US tightening of Iranian sanctions in 2012 was met with a string of systematic Iranian DDoS cyberattacks targeted at US banks and government agencies, affecting “at least 46 financial institutions and companies”;⁸⁰ in 2015 this series of cyberattacks finally came to an end, notably corresponding to the signing of the JCPOA. Iran’s cyber operations resumed a regional focus at this time, with limited identified efforts targeting the US.⁸¹

Bearing Iran’s tight correlation of cyber operations to geopolitics, it is no surprise why members of the security community were and still are concerned about the implications likely to follow the US withdrawal from the JCPOA. As most of the significant Iranian cyber operations targeted at the US took place post-Stuxnet and pre-JCPOA (2011-2015), cybersecurity experts have been fearing that with the end of US participation in the deal, will concurrently come the end of this recent “lull” in Iranian cyberattacks.⁸²

⁷⁸ Walls, “Nation-States: Why They Hack,” 7.

⁷⁹ Walls, “Why Iran Hacks.”

⁸⁰ Andy Greenberg, “The Iran Nuclear Deal’s Unraveling Raises Fears of Cyberattacks.”

⁸¹ Hodgson et. al., 27.

⁸² Andy Greenberg, “The Iran Nuclear Deal’s Unraveling Raises Fears of Cyberattacks.”

At the end of 2018, a *Wired* article suggested “signs that the pushback [had] arrived.”⁸³ It quotes Eric Chien of security firm Symantec’s security and technology division, as he comments on the noticeable “nation state motivations” of Iranian cyber activity, as well as the extent to which it is “reactionary to the geopolitical world.” The recent attacks that have spurred thought that Iran’s state-sponsored hacking has ramped up once again have been tied to Iran largely due to the malware involved - a variant of Iran’s prior multi-use and severely destructive *Shamoon* virus. Separately, another APT group attributed to Iran (Charming Kitten)—known for targeting government and diplomatic sectors⁸⁴—has recently been tied to attacks on US Treasury officials, DC think tanks, and other similarly functioned groups. The murk of attribution remains, but security researchers assert this “spike in Iranian hacking.”⁸⁵

United States and Russia. The Cold War era, lasting until the early 1990’s, was defined by US and (now) Russian bipolar power competition and geopolitical tension. In the post-Cold War era and 21st century, largely comprised of increasing globalization and technological advancement, the US-Russian relationship has not been marked by cooperation, even in the absence of formal tension. Although optimistic sentiments have been made by many US presidents since the end of the Cold War regarding the hope for better relations with Russia, obstacles have continued to prevent this from manifesting. Tensions such as the US intervention and expansion of NATO, have remained fundamental points of contention.

Both the US and Russia have subtly continued the Cold War policy of containment with one another, as Russia attempts to “constrain American commercial advance, America to limit

⁸³ Lily Hay Newman, “The Iran Hacks Cybersecurity Experts Feared May Be Here,” *WIRED Magazine*, December 18, 2018, <https://www.wired.com/story/iran-hacks-nuclear-deal-shamoon-charming-kitten/>

⁸⁴ “Charming Kitten,” *Malpedia*. Accessed November 20, 2019, https://malpedia.caad.fkie.fraunhofer.de/actor/charming_kitten

⁸⁵ Lily Hay Newman, “The Iran Hacks Cybersecurity Experts Feared May Be Here.”

Russian territorial expansion.”⁸⁶ Russia has continued to view US policy as imperialist, disagreeing with their unipolar status and spreading of democracy, while pursuing their own power revival and sphere of influence, beyond their regional confines, and into the global power distribution. The post-Cold War US relatively succeeded in unipolar power dynamics, leading shifts towards multilateral liberal integration and pushes to domestic democracy of others.⁸⁷

More recently, consequential actions from the Russian state have only led to increased tensions. The 2014 Russian invasion of Ukraine and the annexation of Crimea caused relations to “[plummet] to their lowest since the end of the Cold War.”⁸⁸ Soon after in 2016, as will be discussed in this study, the Russian interference in the 2016 US presidential election has also mangled the US-Russian bilateral relationship, resulting in anti-Russian sanctions and a bleak outlook for the near future.⁸⁹ This next section will briefly discuss the key aspects and events from the US-Russia relationship concerning state-level cyber operations.

State-sponsored Cyber Activity. The destabilization and disinformation efforts of Russia’s state-sponsored cyber operations are interwoven, and contribute to each other in order to act on state objectives. Efforts range from political election interference to abuse of social media platforms. In addition to technical cyber operations, Russian state actors have established online personas on varying Internet platforms such as Twitter and Facebook, to “disseminate falsified news stories and develop narratives sympathetic to Russia’s views.”⁹⁰ As the spreading of disinformation on media platforms is largely political in influencing public opinion, it also serves

⁸⁶ Thomas Graham, “U.S.-Russian Relations in a New Era,” *The National Interest*. January 6, 2019.

⁸⁷ Eugene Rumer, and Richard Sokolsky, “Thirty Years of U.S. Policy Toward Russia: Can the Vicious Circle Be Broken?” *Carnegie Endowment for International Peace*, June 20, 2019.

⁸⁸ Ibid.

⁸⁹ Thomas Graham, “U.S.-Russian Relations in a New Era.”

⁹⁰ Hodgson et. al., 9

to undermine credible sources.⁹¹ Since at least 2007, the Russian state-sponsored cyber group APT28 has conducted espionage to gather intelligence on defense and geopolitical issues, with targets including the US.⁹² However, Russian state-sponsored cyber operations extend beyond the scope of espionage; the intrusions and hacking of the 2016 US presidential election (mainly the campaign of Democratic candidate Hillary Clinton) emphasize the unique Russian focus on information operations, sometimes referred to as “weaponization of information.”⁹³

This pivotal operation targeted and penetrated the networks of the US Democratic Party, ultimately stealing sensitive campaign strategy data, discussions, tactics as well as private personal information of campaign officials and their email correspondence, which would then be leaked to multiple websites and outlets (WikiLeaks, DCLeaks). Over 58,000 email messages were published on WikiLeaks alone.⁹⁴ This public release of documents escalated the Russian espionage operation into “something far more menacing: political sabotage,” as stolen data was also published under a fake persona known as Guccifer 2.0, a fabricated Romanian lone-hacker.⁹⁵ Despite these efforts to false-flag identity and distract attribution from the Russian government, the DNC hack was attributed to two different Russian military intelligence branches (FSB, GRU).⁹⁶ It was later revealed that disinformation efforts were happening simultaneously with network intrusion and public data breaching, as Facebook alone announced over 3,000 advertisements posted were linked to Russia during the time surrounding the 2016 presidential

⁹¹ Ed Parsons and Michael Raff, “Understanding the Cyber Threat from Russia.” *F-Secure Cyber Security*, Accessed November 10, 2019, <https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-russia>

⁹² “Foreign Economic Espionage in Cyberspace,” 8.

⁹³ Ben Buchanan and Michael Sulmeyer, “Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration,” *Carnegie Endowment for International Peace*, December 13, 2016.

⁹⁴ “2016 Presidential Campaign Hacking Fast Facts,” *CNN*, October 31, 2019. <https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

⁹⁵ Eric Lipton, David E. Sanger, and Scott Shane, The Perfect Weapon: How Russian Cyberpower Invaded the U.S., *The New York Times*, December 13, 2016, <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>

⁹⁶ Gordan Corera, Can US election hack be traced to Russia? *BBC News*, December 22, 2016, <https://www.bbc.com/news/world-us-canada-38370630>

election.⁹⁷ The aftermath included US indictment of several Russian intelligence and military officials, and the infamous Mueller investigation into Russian interference in the election concluded that Russia was in fact engaging in sophisticated campaigns of both *disinformation* and *destabilization*; in addition to hacking the networks of the Democratic party and campaigns and publishing the material, they additionally “conduct[ed] disinformation and social media operations in the United States designed to sow social discord.”⁹⁸

The Russian actions taken to destabilize the US presidential election and to spread disinformation surrounding it largely correspond to their state objectives of interfering with the western democratic political system, and thus undermining the credibility of western democracy, as Russia has additionally afflicted European countries such as France and Germany with similar cyber tactics.⁹⁹

Russian objectives have largely remained since the Cold War era. During even this time, disinformation campaigns existed in order to undermine and discredit US intelligence and alliances, and to bolster Soviet power and influence, although the methodology was much different (forgery, targeted assassination). Today, cyber operations allow Russia to not only continue strategically acting on their objectives, but to do so in a systematic, technically skilled, covert, difficult-to-trace manner—a manner in which capability and rules remain ill-defined and competitive.¹⁰⁰ Seth Jones, senior advisor to the CSIS, comments on Russian use of “technologically-sophisticated offensive cyber capabilities, covert action, and information operations” in order to not only strengthen their own power, but to also “[contribute] to a decline

⁹⁷ “2016 Presidential Campaign Hacking Fast Facts,” *CNN*.

⁹⁸ Letter from Attorney General William P. Barr to the Honorable Lindsey Graham, the Honorable Dianne Feinstein, the Honorable Jerrold Nadler, and the Honorable Doug Collins, March 24, 2019.

⁹⁹ Hodgson et. al., 9.

¹⁰⁰ Seth G. Jones, “Russian Meddling in the United States: The Historical Context of the Mueller Report,” *Center for Strategic and International Studies*, March 27, 2019.

in American global power and influence.”¹⁰¹ Russian APTs, often branches of Russian military intelligence (FSB, SVR) have targeted commercial companies, government agencies, political parties, and IOs around the world,¹⁰² exemplified by destructive malware such as NotPetya, targeting multinational corporations, for example.¹⁰³ However, Russia exhibits a unique focus on the energy sector in their state-led cyber operations, with a priority especially on power grids and industrial control systems. According to security journalist Steven Musil, national energy, nuclear and other critical infrastructure organizations have become frequent Russian targets “due to their ability to cause immediate chaos, whether it's starting a blackout or blocking traffic signals.” To make matters worse, these critical systems are often inherently “vulnerable because of antiquated software and the high costs of upgrading infrastructure.”¹⁰⁴

Sandworm, a prominent Russian state actor that has been active since at least 2014 (traced to Russian military branch GRU¹⁰⁵), has particularly targeted power grids.¹⁰⁶ Security firm FireEye has linked Sandworm to a string of US energy facility intrusions discovered in 2014, “which were infected with the same Black Energy malware Sandworm would later use in its Ukraine attacks.”¹⁰⁷ Sandworm abruptly carried out attacks on Ukrainian electric utilities in 2015 and 2016, cutting off power to hundreds of thousands of people.¹⁰⁸ The attackers gained control of power distribution and control centers, shutting them down and offline, and going as

¹⁰¹ Ibid.

¹⁰² Hodgson et. al., 10-1.1

¹⁰³ Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *WIRED Magazine*, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

¹⁰⁴ Steven Musil, “Russian hackers accessed US electric utilities' control rooms,” *CNET*, July 24, 2018. <https://www.cnet.com/news/russian-hackers-reportedly-gained-access-to-us-utility-control-rooms/>

¹⁰⁵ Andy Greenberg, “Your Guide to Russia’s Infrastructure Hacking Teams,” *WIRED Magazine*, July 12, 2017, <https://www.wired.com/story/russian-hacking-teams-infrastructure/>

¹⁰⁶ “Sandworm Team,” *Mitre*, Accessed November 20, 2019, <https://attack.mitre.org/groups/G0034/>

¹⁰⁷ Andy Greenberg, “Your Guide to Russia’s Infrastructure Hacking Teams.”

¹⁰⁸ Ibid.

far as to even disable backup power supply.¹⁰⁹ This was the first ever blackout or outage attack; although targeting Ukraine, it immediately raised concerns in the US, as experts still claim this bold move was in fact a “flex” of Russian cyber capability, perhaps in order to present their persistent threat to the US. These concerns proved valid, as Russian cyber activity on US grids has continued and increased since these preliminary outage attacks on Ukraine. A 2018 DHS Cyber + Infrastructure alert shed light on Russian state cyber activity that had “staged malware, conducted spear phishing, and gained remote access into energy sector” and other sensitive critical infrastructure networks, as well as “conducted network reconnaissance, moved laterally, and collected information pertaining to [US] Industrial Control Systems” after attaining access.¹¹⁰ Targets included government facilities, as well as a nuclear plant, and multiple power plants.¹¹¹

However, this unauthorized access goes both ways. It is important to note that the US has been probing Russian infrastructure since at least 2012, mainly by conducting reconnaissance into the Russian electric grid. More recently, the US has been admittedly more aggressive in their approach to “defending forward” by implanting malware inside Russia’s state control systems.¹¹² Neither Russia nor the US has gone as far as to actually shut off the power of each other’s grids; only the “persistent threat” of the others’ capability remains, which has thus stirred dialogue about a new “digital cold war.”¹¹³ Yet in a domain of warfare that is loosely defined and

¹⁰⁹ Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *WIRED Magazine*, March 2, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

¹¹⁰ “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors,” *Cyber + Infrastructure, Department of Homeland Security*, March 15, 2018, <https://www.us-cert.gov/ncas/alerts/TA18-074A>

¹¹¹ Jennifer Dlouhy and Michael Riley, “Russian Hackers Attacking U.S. Power Grid and Aviation, FBI Warns,” *Bloomberg*, March 15, 2018.

¹¹² David E. Sanger and Nicole Perloth, “U.S. Escalates Online Attacks on Russia’s Power Grid,” *The New York Times*, June 15, 2019, <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>

¹¹³ Marc Champion, “Digital Cold War,” *The Washington Post*, May 20, 2019, https://www.washingtonpost.com/business/digital-cold-war/2019/05/17/2f01effa-7895-11e9-a7bf-c8a43b84ee31_story.html

barely legitimized, deterrence is not as clearly interpreted. Targeting specifically the Ukraine and the US (and European countries to a lesser extent) epitomizes a challenging of western influence on neighboring countries and the West as an entity.

Based on actions taken in the cyberspace domain, as expert Mike Walls suggests, it is “conceivable that Russian officials view hacking, or more appropriately cyberwarfare, as a political tool which, when employed, is extremely effective at helping a nation state achieve a geopolitical goal.”¹¹⁴ A 2017 article published by the University of Washington’s School of International Studies agrees with the link between Russian cyber operations and its geopolitical objectives, suggesting “while Russia is concerned about Ukraine turning to the West, it is also concerned with Ukraine’s moves to end its dependence on Russian energy sources.”¹¹⁵

Objectives deduced from Russian strategy and cyber operations indicate a focus to to 1) undermine Western influence, and 2) target the energy industry.¹¹⁶

National security correspondent David Sanger suggests the motives for American probing into Russian control systems as serving “partly as a warning, and partly to be poised to conduct cyber strikes if a major conflict broke out between Washington and Moscow.”¹¹⁷ This judgment aligns with the concept of attempting to “hold targets at risk” as well as being prepared for retaliation *or* an offensive cyberattack if tension in the bilateral relationship were to intensify. Whether preparation for retaliation or offensive attack, the capability of Russian access into critical infrastructure could still serve as a legitimate threat and display of power and presence.

¹¹⁴ Walls, “Nation-States: Why They Hack,” 5.

¹¹⁵ Donghui Parks,, Julia Summers and Michael Walstrom. “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.” *The Henry M. Jackson School of International Studies, The University of Washington*. October 11, 2017.

¹¹⁶ Ibid.

¹¹⁷ David. E. Sanger and Nicole Perloth. “U.S. Escalates Online Attacks on Russia’s Power Grid”

Cyber Conflict: What Makes It Unique?

After an overview of the four leading cyber powers' approaches to cyber strategy and cyber conflict in regards to their bilateral relationships, we can begin to examine the intrinsic qualities of cyber conflict that exist across different methods, objectives, or state actors. Doing so will encourage later discussion on how cyber conflict fundamentally interacts with the LIO.

The goal of this section is to explore what makes cyber conflict a uniquely new challenge for nation-states, by drawing from relevant literature as well as from this paper's case studies on US-China, US-Iran, and US-Russia. Nazli Choucri, director of the multi-disciplinary ECIR MIT-Harvard research collaboration, has significantly contributed to defining key characteristics of cyberspace, which she insists are "reshaping contemporary international relations theory, policy, and practice."¹¹⁸ These seven attributes, (seen in Appendix E) include 1) temporality 2) physicality, 3) permeation, 4) fluidity, 5) participation, 6) attribution, and 7) accountability.¹¹⁹

Time and space, evident in the first two of Choucri's characteristics of cyberspace, are two of the most prominent ways in which cyber conflict is unique from kinetic conflict. As also evidenced by Segal in his distinction of cyber espionage (from traditional espionage), "[cyber espionage] is easier, happens at a much greater pace, and produces a greater haul," and while "industrial espionage happened over years and decades; cyber espionage takes place over hours and days."¹²⁰ Additionally, the very nature of "zero-day exploits" as advanced cyberattacks are defined by their temporal aspect; these attacks are exploitations of unknown vulnerabilities to the developer until they are exposed, giving them zero days to patch the vulnerability.¹²¹

¹¹⁸Choucri, Nazli, "Cyberpolitics in International Relations," (*The MIT Press: Cambridge, Massachusetts*, 2012): 3

¹¹⁹ Ibid., 4.

¹²⁰ Segal, 153.

¹²¹ "What is a Zero Day Exploit?" *Kaspersky*, <https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit>

In terms of physicality, cyber operations obviously are not physical in nature, as kinetic warfare and battlefield warfare are. The ability of cyber weapons to “transcend constraints of geography and physical location” allows for efforts such as persistent engagement on an adversary’s network, and reconnaissance (an advanced form of targeted spying; the first step in the cyberattack *cyber kill chain*, closely defined to espionage¹²²).¹²³ If intended for espionage, persistent access on a system can allow an easy entry to stealing data and gathering intelligence; additionally, it can be utilized to scope out the virtual landscape of an attack target. Admiral Mike McConnell comments on the potential of remote exploit or attack on critical networks and information, in which “no flotilla of ships or intercontinental missiles or standing armies can defend against such remote attacks located not only well beyond our borders, but beyond physical space, in the digital ether of cyberspace.”¹²⁴ This point also speaks to the asymmetry of cyberwarfare; unlike conventional war methods, this conflict doesn’t require large nation-state militias, and is instead more typically technically-skilled individual actors working for a government that could theoretically have the ability to shut down a grid system.¹²⁵

The phenomenon of malware recycling is unique to cyber conflict, and encompasses both the *permeation* and *fluidity* aspects outlined by Choucri. When a nation-state launches a missile, or engages in battleground warfare with an opposing state, those strategies and tools aren’t repurposed for later use by other states or actors. In state-level cyber operations, however, malware, ransomware, viruses, are often deconstructed by various entities (security researchers and firms along with the government) and pieces of the code are dissected, whether for understanding the adversary’s capabilities, or for patching vulnerabilities, but different segments

¹²² “The Cyber Kill Chain,” *Lockheed Martin*.

¹²³ Nazli Choucri, “Cyberpolitics in International Relations,” 4.

¹²⁴ Richard A. Clarke and Robert K. Knake, “Cyber War The Next Threat to National Security and What to Do About It,” 2010.

¹²⁵ *Ibid.*

of malware can be sold and used again, as has been seen in even nation-state cyber conflict. The US-Israeli-made Stuxnet worm, as discussed in the US-Iran case study of this thesis, has been repurposed for acting on vastly different objectives. A 2013 NSA document leaked by Snowden indicates concern and evidence that Iran demonstrated replicated techniques from US malware such as Stuxnet, Flame, and Duqu in their well-known Shamoon malware.¹²⁶ Shamoon is also an example of an attack that has been modified by its creators to strike again, at different targets; according to firm FireEye, the 2018 “Shamoon 2.0 [was] a reworked and updated version of the malware [they] saw in the 2012 incident.”¹²⁷ This challenge, unique to cyberwarfare, is one of the many new challenges that has emerged with the rise of cyber as a fifth domain of warfare.

Participation and *attribution* contribute to the opaqueness of cyber operations as well. Although not the focus of this thesis, non-state actors with sophisticated technical skills (and at times hired to execute governments’ cyber operations) blur the lines between state cyber operations and non-state cybercrime, and present a unique challenge for nation-states combatting and responding to this type of attack. Specific to the *problem of attribution*, while identifying the actor behind malware campaigns and cyberattacks is a unique challenge of its own, “false-flagging” is also employed by sophisticated state APT actors in order to deceive and mislead victims and the security community from correctly identifying the origin or identity of the attack. Exemplified in this paper’s case study on US-Russia, as Russia publicly denied any involvement during their DNC and US election hacking campaign, they intentionally disguised their identity with a false persona of Romanian origin.¹²⁸ *Accountability* goes hand-in-hand with the challenge

¹²⁶ Kim Zetter, “The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks,” *WIRED Magazine*, February 10, 2015, <https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/>

¹²⁷ “FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region,” *FireEye*, December 1, 2016, https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html

¹²⁸ Andy Greenberg, “Russian Hacker False Flags Work-Even After They’re Exposed,” *WIRED Magazine*, February 27, 2018, <https://www.wired.com/story/russia-false-flag-hacks/>

of identifying and responding to cyber conflict, in ways it would not in conventional warfare. Naturally, as correct attribution is difficult already, it is especially difficult to hold states accountable for malware campaigns they only allegedly were behind. It is difficult to be held accountable for cyber activity in the same way one may be for developing or testing nuclear weapons, for example, as this approach to warfare does not require huge physical development facilities or physically detectable testing.

The nature of certain cyber operations such as persistent engagement, network penetration, probing and reconnaissance—as mentioned above when examining the temporal and physical aspect of cyber conflict—also present a challenge while distinguishing benign, defensive cyber activity from that of reconnaissance efforts in preparation for a targeted malicious cyberattack. Active defense measures or monitoring can look very similar to conducting reconnaissance, raising unprecedented questions such as whether or not reconnaissance efforts should be treated like an attack, or how to respond to Russian or US electrical grid probing and access to networks. Misinterpretation of another state’s activities in cyberspace, or misattribution of attacks or operations could very possibly lead to escalation, “especially if a malicious or self-interested actor were to route attacks on the other side through US or Chinese servers during a tense period in the bilateral relationship,” for example.¹²⁹ These potential conflicts blur wartime and peacetime, and elucidate the gaps (or even irrelevancy) in traditional definitions of offensive and defensive state behavior.

Cyber Conflict and the Liberal International Order

¹²⁹ Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "The “Cyber Problem” in U.S.-China Relations," In *Getting to Yes with China in Cyberspace*, 8. Santa Monica, Calif.: RAND Corporation, 2016.

Recent literature suggests the liberal international order (LIO) is evolving, and is no longer the postwar system that it was once in the 20th century.¹³⁰ Further, some experts argue it is in crisis.¹³¹ Some such as the prominent scholar on American international relations John Mearsheimer have presented evidence even indicating the end of the LIO.¹³² Despite consensus on the declining or expired health of the liberal order, there are certain undeniable facts of the current world stage and geopolitical climate that challenge the pillars of this US-led, rule-based order, which are traditionally defined as democracy, open markets, multilateral cooperation, security alliances, international institutions and U.S. hegemony.¹³³

Current challenges have risen to fundamentally oppose the inherent system of the liberal international order. For example, the 2008 and Eurozone crises served to challenge the underlying assumptions and arguments of the true feasibility of the LIO, by revealing intrinsic flaws of the open self-regulating market. Another threat to this open system is the “return to great-power rivalry,” which senior fellow at the Brookings Institute and author Thomas Wright argues was inevitable. He claims that growing “geopolitical competition” amongst world powers such as China and Russia have contributed to the “clash of social models” coming to a head; after decades of interconnectedness and integration encouraged by the liberal order, global powers have vulnerabilities.¹³⁴

Similar to Wright, Mearsheimer claims that despite the once strong existence of the LIO, it “contained the seeds of its own ruin” from the start. Former Prime Minister of Sweden acknowledges the crisis of the LIO as well by illuminating key countries’ “isolationist

¹³⁰ Hanns W. Maull, “The Once and Future Liberal Order,” *The International Institute for Strategic Studies. Survival: Global Politics and Strategy April–May 2019* 2, no. 61 (March 2019).

¹³¹ John G. Ikenberry, “The Liberal International Order and its Discontents,” (2010).

¹³² John J. Mearsheimer, “Bound to Fail: The Rise and Fall of the Liberal International Order,” *International Security*, 2019.

¹³³ John G. Ikenberry, “Power and Liberal Order: America’s Postwar World Order in Transition,” 2005.

¹³⁴ Thomas Wright, “The Return to Great-Power Rivalry was Inevitable,” *Brookings Institute*, September 12, 2018.

sentiments” and revisionist powers becom[ing] more assertive,” as well as the “questioning of free trade and the open global economy.”¹³⁵ Senior distinguished fellow of the German Institute for International and Security Affairs Hanns Maull adds to this, suggesting that the advance of technology is the primary “driver of disorder” of the liberal global order, along with the “supply-demand in governance” and “eroding international cooperation.”¹³⁶

Other evidence includes the rise of domestic populist national movements such as Brexit, the declining public trust in government, and the election of other populist and nationalist leaders. Donald Trump in the US has strayed from supporting basic principles of the LIO; as the president of the supposed hegemon of this world order, his election raises questions about the continuity and stability of the order today, as does China’s emergence as a potential leader, while lacking a democracy and instead engaging with an authoritarian government. This thesis will introduce nation-state cyber operations and conflict as another “driver of disorder” that is beginning to additionally visibly challenge the liberal international order.

Power shift. Firstly, many of the emerging and established cyber powers the world has witnessed in the last decade are not only non-western or non-democratic, but have been characterized as being *anti-democratic* and *anti-western*. China and Russian particularly have challenged US hegemony since long before this decade. Both non-Western states, they do not subscribe to the same liberal principles of democracy that the West has for quite some time. Iran is an Islamic republic, and in this way does not subscribe to secular principles of liberalism. All three of these states have demonstrated their power struggles with the LIO in different forms, whether by the threat of nuclear weapon development, or economic challenges. In challenging US hegemony and exerting their own differing spheres of influence in contrast to Western influence, they have

¹³⁵ Judy Dempsey, “Judy Asks: Is the Crisis of the Liberal Order Exaggerated?” *Carnegie Europe*, February 18, 2017.

¹³⁶ Hanns W. Maull, “The Once and Future Liberal Order.”

sought a multipolar global power distribution rather than one of US-led unipolarity. A rise of these actors, via cyber advancement and superiority, and thus a shift towards a multipolar distribution, would certainly challenge US hegemony and traditional trademark features of the LIO — whether it continues or not.

Openness of the LIO. As discussed previously, cyberattacks are increasingly difficult to attribute (especially with the rise of false-flagging), and this can cause serious issues when placing internationally public blame or responsibility on another nation-state. Moreover, if governments are able to execute attacks and escape attribution, there is very little incentive for states to subscribe to policies of transparency and accountability. The lack of this type of international agreement challenges the liberal openness and accountability that has surrounded battlefield warfare and large-scale military campaigns for decades. The problem of attribution threatens the accountability that is essential to international cooperation in the LIO.

Additionally, this renders cyber conflict intrinsically more difficult to regulate by an IO, which has largely been the approach to handling international conflict within the LIO. IOs regulate everything from trade, tariffs, and sanctions to the establishment of acts of aggression, and appropriate responsive measures. The lack of legitimate agreement and difficulty of attribution poses a threat of undermining the fundamentals of the LIO. Without transparency, how will IOs continue to monitor state conflict? When a nation tests a missile, the world knows almost immediately; when a nation constructs physical facilities for nuclear weapon development, other states or IOs can physically observe this and monitor it. However, when a nation tests a piece of malware, there is little to no way of knowing; when a nation begins ramping up their cyber capability, this goes unknown until execution of sophisticated attacks, or until malware is attributed to that state actor. One of the conditions of the 2016 JCPOA was IO

routine monitoring on Iran's nuclear development in order to keep Iran accountable and compliant, however, is this regulation possible in an era of cyber tools and writing malware? The lack of physical equipment renders this method of ensuring accountability in cyber conflict much more difficult. Yet further, if the international community cannot reliably attribute attacks, there is no perpetrator to hold accountable in the first place. Without fear of facing repercussions and being held accountable from the global community and/or established international liberal institutions, such as the UN and IOs, there seems to be little that prevents a nation from developing and using these capabilities, especially if they can get away with it not being attributed. Irony lies in the LIO's ideals of maintaining an open, integrated, interconnected system. Technology has allowed for this integration to happen, however this openness is now being exploited by technologically sophisticated methods to undermine and challenge the LIO, and the principles that it was built from.

Hegemonic correspondence to military strength. Global military primacy is a defining characteristic of US hegemony in the LIO, as military strength often corresponds to effective state hegemony. According to the Hegemonic Stability Theory (HST), the political power of a hegemon must be "backed up by projective military power."¹³⁷ This characteristic assumes "strength both politically and economically" as well, as resources are necessary to maintain an unrivaled military.¹³⁸ Because state cyber operations and cyberattacks need not a hugely-resourced and organized, physical army or the legitimacy of a well-funded public state military, cyber operations challenge the underlying notion that military strength is directly corresponding to global power and hegemonic status. Cyberattacks are relatively much cheaper than traditional

¹³⁷ Vincent Ferraro, "The Theory of Hegemonic Stability," <https://www.mtholyoke.edu/acad/intrel/pol116/hegemony.htm>.

¹³⁸ N. M. Yazid, "The Theory of Hegemonic Stability, Hegemonic Power and International Political Economic Stability."

kinetic military campaigns.¹³⁹ In addition, governments have been known to use non-state actors to execute their state-*led* operations, leveraging their experience and technical skills to attain cyber capability and potentially “wage war against an enemy with kinetic battlefield superiority.”¹⁴⁰ Thus, cyber operations prove a way to challenge the position of the hegemon in ways kinetic warfare cannot. In the same vein, hegemonic states are generally assumed to have the more developed and advanced infrastructure relative to the rest of the world, as they are capable enough to provide public goods for other nations and have a large economy.¹⁴¹ However, this “traditional power dynamics are undermined by the paradoxical idea that the most technologically advanced countries are also the most dependent on digital infrastructure which is inherently more susceptible to flaws and vulnerabilities in CNI, “and thus the most vulnerable to a crippling cyber-attack.”¹⁴² Porche comments that “open and free societies are more vulnerable than adversaries who exploit the tenets and principles of press freedoms.”¹⁴³ These aspects challenge the traditionally-held military superiority of the hegemonic state in the LIO; cyber conflict presents opportunities for less powerful, smaller and less-resourced governments to exploit vulnerabilities of advanced systems within powerful nations, and thus challenge the role of the hegemon in ways it could previously not. This is seen in each of the three case studies, as China, Iran and Russia have gained the attention and concern from the US, as all three have successfully engaged in some extent of cyber operations targeted at the US. Cyber conflict allows for this type of *asymmetric* warfare; prior to cyber operations, smaller and

¹³⁹ Naushad K. Cherrayil, “State-sponsored actors to launch more coordinated cyber attacks.”

¹⁴⁰ Johan Sigholm, “Non-State Actors in Cyberspace Operations” (2016) <https://doi.org/10.1515/jms-2016-0184>.

¹⁴¹ Vincent Ferraro, “The Theory of Hegemonic Stability,” <https://www.mtholyoke.edu/acad/intrel/pol116/hegemony.htm>.

¹⁴² Anthony J.S. Craig and Brandon Valeriano, “Realism and Cyber Conflict: Security in a Digital Age,” 2018.

¹⁴³ Isaac Porche, “Getting Ready to Fight the Next (Cyber) War.”

less-resourced or legitimate forces would rarely, if ever, conduct offensive operations targeting the world's largest military.

Rules-based, but no rules. Defining offensive and defensive behavior challenges the rules-based nature of the order. The LIO is largely defined as a rules-based international order. In the LIO era, war is formally (usually) declared and there are international laws surrounding fair targets and what constitutes an act of war or aggression, and how a nation can respond. Until there is comprehensive work and agreement that addresses interpreting grey area threats such as reconnaissance of network intrusion or power grid probing, this characteristic of cyber conflict will undermine the liberal institutions and their ability to regulate conflict on an international scale, and thus the LIO at large.

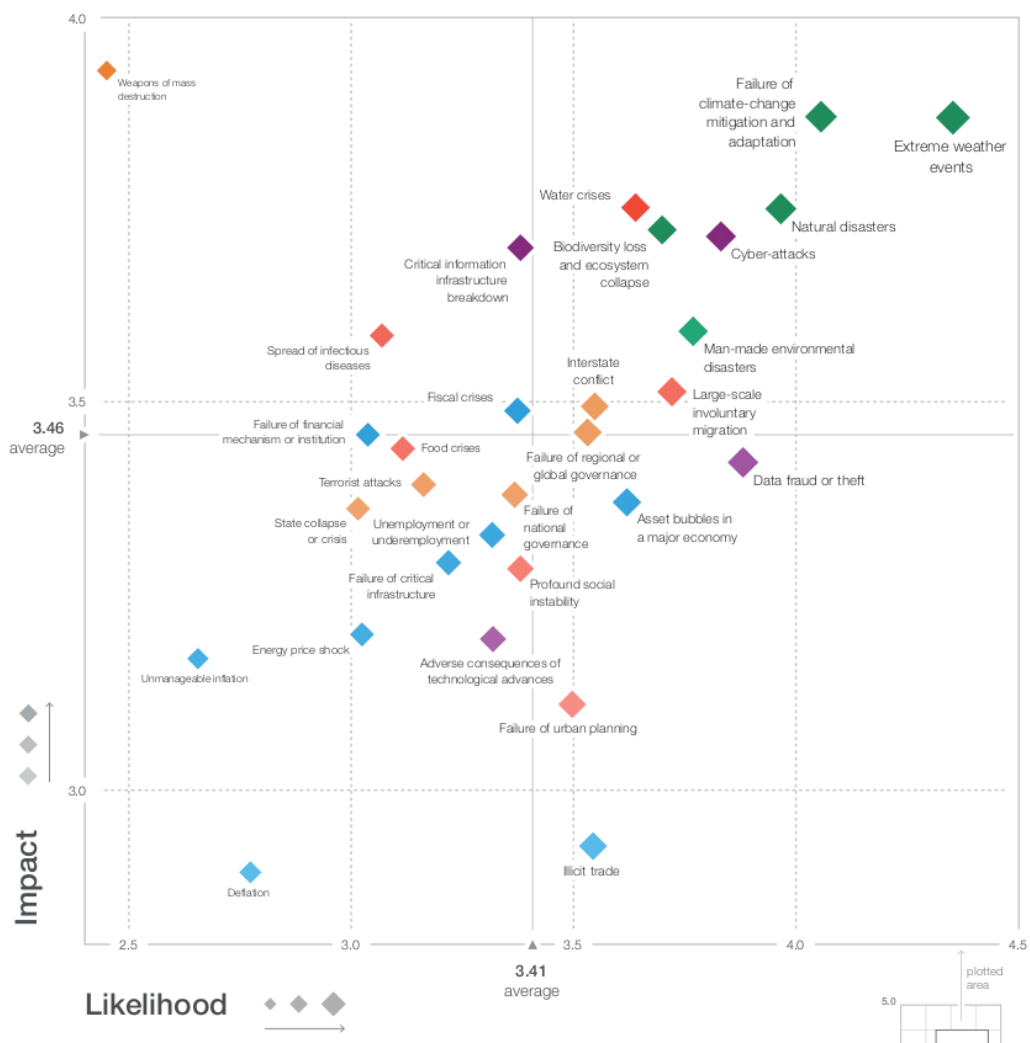
To again reference Choucri's contribution to cyber international relations, she ultimately asserts the "co-evolution of cyber domain and international relations," which the research and analysis presented in this thesis supports as well. Inherent features of cyber operations and conflict challenge the current LIO, and will continue to shape its future. As this thesis has presented evidence that cyber conflict challenges the LIO in ways that kinetic warfare does not, it additionally supports Choucri's reverse argument, specifically that geopolitics continue to serve as a major objective of state cyber operations, as demonstrated in each of the three case studies. Thus, these two seemingly separate realms are largely intertwined and continue to co-evolve.

Conclusion

Whether or not the future nature of state warfare shifts towards one of largely cyber, or a mix of both methods, or whether or not a cyberwar causes comparable damage to kinetic wars in the future, that is not for this thesis to suggest. However, based on the increasing prevalence and

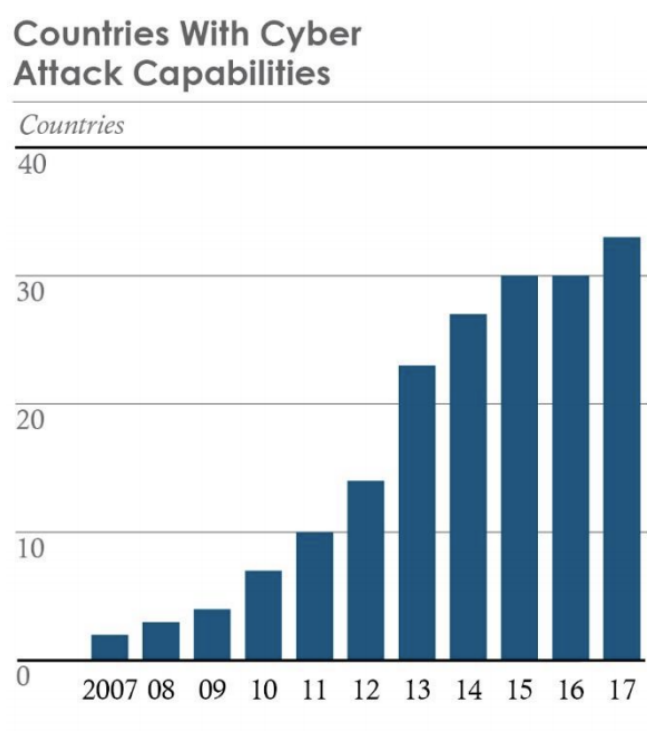
severity of state cyber operations, it is fair to say that state cyber operations warrant concern and prioritization of this topic within technical fields *as well as* international studies. Despite the future of state warfare, there are inherent and fundamental characteristics of cyber conflict that render it an entirely unique challenge than previous forms of military kinetic battlefield warfare. These qualities are evident based on state cyber operations within US bilateral relationships of the last decade, especially those that were focused on in this thesis. Lastly, and for the most significant contribution to the existing body of literature, not only are these inherent characteristics of state cyber conflict affecting and co-evolving with geopolitics and state relations, but they are directly challenging the stability and continuity of the western-led liberal international order. As other scholars have suggested, the US will have to take various strides in order to preserve the liberal institutions that define its hegemony; however in addition, addressing this new challenge of state-led cyber operations and cyber approaches to warfare will be a must.

Appendix A



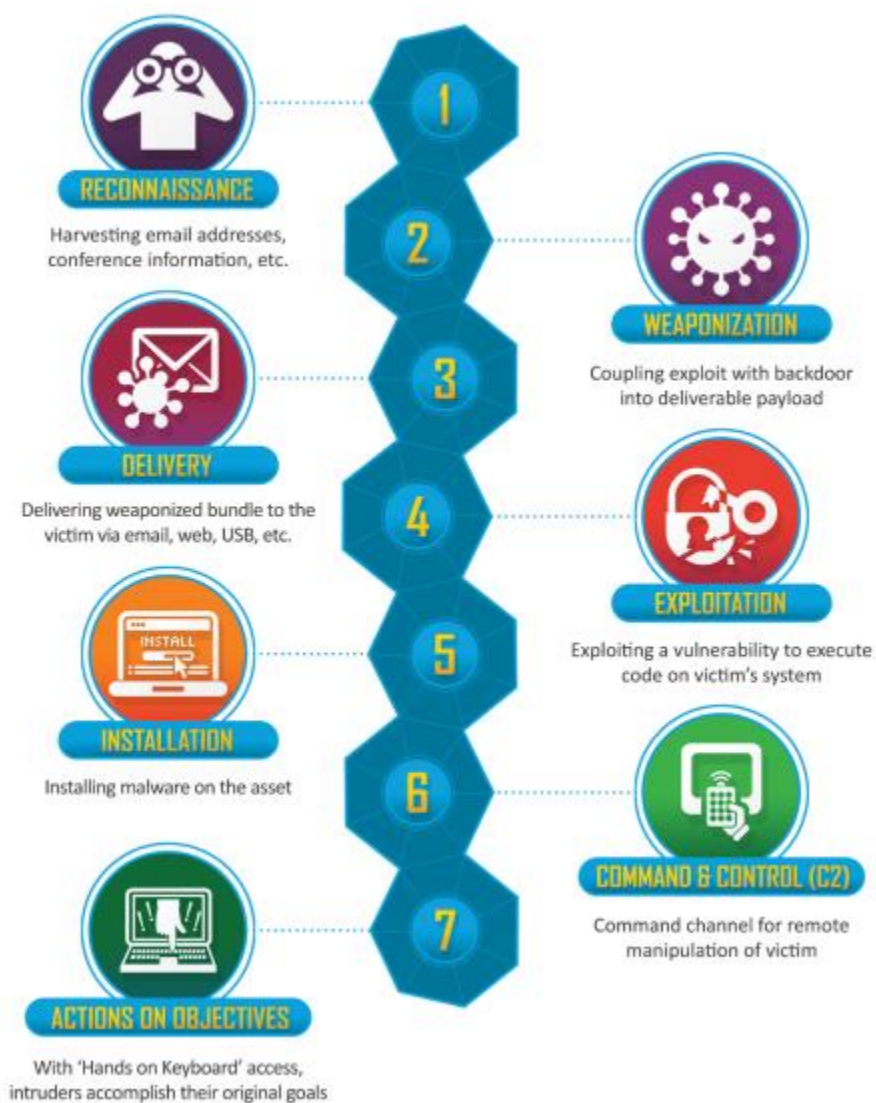
Appendix A: WEF Global Risks Report, 2019.

Appendix B



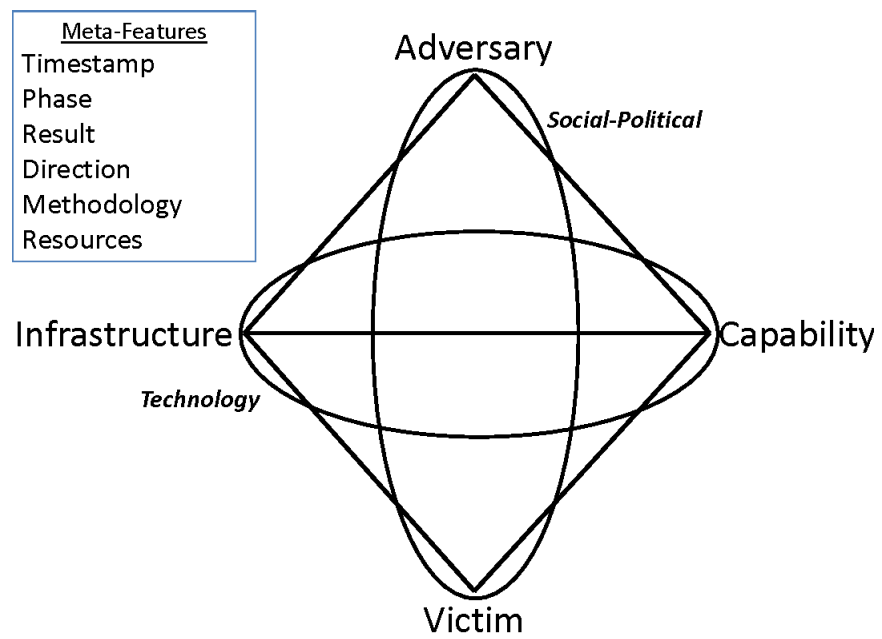
Appendix B: Worldwide Threat Assessment by U.S. Intelligence, 2018.

Appendix C



Appendix C: The Cyber Kill Chain, Lockheed Martin.

Appendix D



Appendix D: The Diamond Model of Intrusion Analysis, 2013.

Appendix E

Characteristics of cyberspace

- *Temporality*—replaces conventional temporality with near instantaneity
 - *Physicality*—transcends constraints of geography and physical location
 - *Permeation*—penetrates boundaries and jurisdictions
 - *Fluidity*—manifests sustained shifts and reconfigurations
 - *Participation*—reduces barriers to activism and political expression
 - *Attribution*—obscures identities of actors and links to action
 - *Accountability*—bypasses mechanisms of responsibility
-

Appendix E: Characteristics of Cyberspace, Nazli Choucri 2012.

Bibliography

“APT1: Exposing One of China’s Cyber Espionage Units.” *Mandiant*. Accessed November 12, 2019. <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

Attorney General’s Letter to House and Senate Judiciary Committee, March 24th, 2019. <https://www.justice.gov/ag/page/file/1147981/download>

Beehner, Lionel. “Timeline: U.S.-Iran Contacts.” *Council on Foreign Relations*. March 9, 2007. <https://www.cfr.org/background/timeline-us-iran-contacts>

Bremmer, Ian. “These 5 Facts Explain the Threat of Cyberwarfare.” *TIME Magazine*. June 19, 2015. <https://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/>

Buchanan, Ben and Michael Sulmeyer. “Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration.” *Carnegie Endowment for International Peace*. December 13, 2016. <https://carnegieendowment.org/2016/12/13/russia-and-cyber-operations-challenges-and-opportunities-for-next-u.s.-administration-pub-66433>

Burgess, Matt. “Is China Really Using Huawei to Hack the World’s Communications?” *WIRED Magazine*. January 25, 2019. <https://www.wired.co.uk/article/huawei-5g-uk-security>

Caltagirone, Sergio, Christopher Betz, and Andrew Pendergast. “The Diamond Model of Intrusion Analysis.” *Center for Cyber Threat Intelligence and Threat Research*. July 5, 2013. <http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

Calmes, Jackie, and Steven Lee Myers. “U.S. and China Move Closer on North Korea, but Not on Cyberespionage.” *The New York Times*. June 8, 2013. <https://www.nytimes.com/2013/06/09/world/asia/obama-and-xi-try-building-a-new-model-for-china-us-ties.html>.

Cassell, Bryan-Low et al. "Special Report - Hobbling Huawei: Inside the U.S. War on China's Tech Giant." *Reuters*. May 21, 2019. <https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-us-war-on-chinas-tech-giant-idUSKCN1SR1EU>

Chang, Amy. "Warring State: China's Cybersecurity Strategy." *Center for a New American Security*. (December 2014):1-44. <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Warring%20State%20-%20China%27s%20cybersecurity%20strategy.pdf>

"Charming Kitten." *Malpedia*. Accessed November 20, 2019. https://malpedia.caad.fkie.fraunhofer.de/actor/charming_kitten

Choucri, Nazli. "Cyberpolitics in International Relations." *The MIT Press: Cambridge, Massachusetts*. 2012.

Choucri, Nazli. "Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University." *MIT Political Science Department Research Paper* no. 2016-1. <http://dx.doi.org/10.2139/ssrn.2727414>

Choucri, Nazli and David D. Clark. "International Relations in the Cyber Age: The Co-Evolution Dilemma." Cambridge: *MIT Press*, 2019. <https://ieeexplore.ieee.org/servlet/opac?bknumber=8671655>

Chumley, Cheryl K. "Iranian hackers sucker punch U.S. defense officials with creative social-media scam." *The Washington Times*. May 29, 2014. <https://www.washingtontimes.com/news/2014/may/29/iranian-hackers-sucker-punch-us-defense-heads-crea/>

Richard Clarke, "War From Cyberspace," *Center for the National Interest*, December 22, 2009, <https://nationalinterest.org/article/war-from-cyberspace-3278>

Champion, Marc. "Digital Cold War." *The Washington Post*. May 20, 2019. https://www.washingtonpost.com/business/digital-cold-war/2019/05/17/2f01effa-7895-11e9-a7bf-c8a43b84ee31_story.html

Cimpanu, Catalin. Iranian Hackers Charged in March Are Still Actively Phishing Universities. *BleepingComputer*. August 24, 2018. <https://www.bleepingcomputer.com/news/security/iranian-hackers-charged-in-march-are-still-actively-phishing-universities/>

Clarke, Richard A. and Robert K. Knake. "Cyber War The Next Threat to National Security and What to Do About It." Harper Collins e-books: 2010,140.

Coats, Daniel R. "Worldwide Threat Assessment of the US Intelligence Community." *Office of the Director of National Intelligence*. January 29, 2019. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>

Coats, Daniel R. "Worldwide Threat Assessment of the US Intelligence Community." *Office of the Director of National Intelligence*. February 13, 2018. <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>

"Compromise of Saudi Aramco and RasGas." *Council on Foreign Relations*. Accessed November 12, 2019. <https://www.cfr.org/interactive/cyber-operations/compromise-saudi-aramco-and-rasgas>

Corera, Gordan. Can US election hack be traced to Russia? *BBC News*. December 22, 2016. <https://www.bbc.com/news/world-us-canada-38370630>

Craig, Anthony J.S. and Valeriano, Brandon. "Realism and Cyber Conflict: Security in a Digital Age." *Realism in Practice*. (2018): 85-101. <http://www.e-ir.info/wp-content/uploads/2018/01/Realism-in-Practice-E-IR.pdf#page=100>

"Cylance Operation Cleaver Report." *Cylance*. December 23, 2016. https://www.cylance.com/content/dam/cylance/pdfs/reports/Cylance_Operation_Cleaver_Report.pdf

Daniels, Jeff. "Chinese theft of sensitive US military technology is still a 'huge problem,' says defense analyst." *CNBC News*. November 8, 2017. <https://www.cnbc.com/2017/11/08/chinese-theft-of-sensitive-us-military-technology-still-huge-problem.html>

Dempsey, Judy. "Judy Asks: Is the Crisis of the Liberal Order Exaggerated?" *Carnegie Europe*. February 18, 2017. <https://carnegieeurope.eu/strategieurope/68041>

Dlouhy, Jennifer and Michael Riley. "Russian Hackers Attacking U.S. Power Grid and Aviation, FBI Warns." *Bloomberg*. March 15, 2018. <https://www.bloomberg.com/news/articles/2018-03-15/russian-hackers-attacking-u-s-power-grid-aviation-fbi-warns>

Ferraro, Vincent. "The Theory of Hegemonic Stability." *Mount Holyoke College*. Accessed November 12, 2019. <https://www.mtholyoke.edu/acad/intrel/pol116/hegemony.htm>.

Finkle, Jim. "Researchers say Stuxnet was deployed against Iran in 2007." *Reuters*. February 26, 2013. <https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226>

"FireEye Responds to Wave of Destructive Cyber Attacks in Gulf Region." *FireEye*. December 1, 2016. https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html

"Foreign Economic Espionage in Cyberspace." *National Counterintelligence and Security Center*. (July 2018): 1-20. <https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf>

Geers, Kenneth et al. "WORLD WAR C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks." *FireEye*. (2014): 1-22. <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-wwc-report.pdf>

Graham, Thomas. "U.S.-Russian Relations in a New Era." *The National Interest*. January 6, 2019. <https://nationalinterest.org/feature/us-russian-relations-new-era-40637>

Halpern, Michah. "Iran Flexes Its Power by Transporting Turkey to the Stone Age." *The Observer*. April 22, 2015. <https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/>

Harold, Scott Warren, Martin C. Libicki, and Astrid Stuth Cevallos. "The "Cyber Problem" in U.S.-China Relations." In *Getting to Yes with China in Cyberspace*, 1-16. Santa Monica, Calif.: RAND Corporation, 2016. www.jstor.org/stable/10.7249/j.ctt1cx3vfr.6

Hodgson, Quentin E., Logan Ma, Krystyna Marcinek, and Karen Schwindt, "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace." Santa Monica, CA: *RAND Corporation*, 2019. <https://doi.org/10.7249/RR2961>

"How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World." *White House Office of Trade and Manufacturing Policy*. (June 2018): 1-36. <https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf>

Ikenberry, G. John. "The Liberal International Order and its Discontents." *Millennium-journal of International Studies - MILLENNIUM-J INT STUD*. 38. (2010): 509-521. 10.1177/0305829810366477.

Ikenberry, G. John. "Power and Liberal Order: America's Postwar World Order in Transition." *International Relations of the Asia-Pacific* 5, no. 2 (January 1, 2005): 133–52. <https://doi.org/10.1093/irap/lci112>.

"Iran's Cyber Threat: Timeline." *Carnegie Endowment for International Peace*. January 4, 2018. <https://carnegieendowment.org/2018/01/04/iran-s-cyber-threat-timeline-pub-75145>

Isikoff, Michael. "Chinese hacked Obama, McCain campaigns, took internal documents, officials say." *NBC News*. June 10, 2013. <http://www.nbcnews.com/id/52133016/t/chinese-hacked-obama-mccain-campaigns-took-internal-documents-officials-say/#.Xfcu5ufYrBJ>

Jones, Seth G. "Russian Meddling in the United States: The Historical Context of the Mueller Report." *Center for Strategic and International Studies*. March 27, 2019. <https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report>

Greenberg, Andy. "Russian Hacker False Flags Work-Even After They're Exposed." *WIRED Magazine*. February 27, 2018. <https://www.wired.com/story/russia-false-flag-hacks/>

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED Magazine*. August 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

Greenberg, Andy. "The Iran Nuclear Deal's Unraveling Raises Fears of Cyberattacks." *WIRED Magazine*. May 5, 2018. <https://www.wired.com/story/iran-nuclear-deal-cyberattacks/>

Greenberg, Andy. "The WIRED Guide to Cyberwar." *WIRED Magazine*. August 23, 2019. <https://www.wired.com/story/cyberwar-guide/>

Greenberg, Andy. "Your Guide to Russia's Infrastructure Hacking Teams." *WIRED Magazine*. July 12, 2017. <https://www.wired.com/story/russian-hacking-teams-infrastructure/>

Langner, R.. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security & Privacy* 9 (2011): 49-51.

Liberto, Daniel. "Economic Espionage." *Investopedia*. July 29, 2019. <https://www.investopedia.com/terms/e/economic-espionage.asp>

Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." *The New York Times*. December 13, 2016. <https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html>

Mauil, Hanns W. "The Once and Future Liberal Order." *The International Institute for Strategic Studies. Survival: Global Politics and Strategy April–May 2019* 2, no. 61 (March 2019): 7-32. <https://www.iiss.org/publications/survival/2019/survival-global-politics-and-strategy-aprilmay-2019/612-02-mauil>

Mearsheimer, J. John. "Bound to Fail: The Rise and Fall of the Liberal International Order". *International Security* 43, no. 4 (2019): 7-50.

Musil, Steven. "Russian hackers accessed US electric utilities' control rooms." *CNET*. July 24, 2018. <https://www.cnet.com/news/russian-hackers-reportedly-gained-access-to-us-utility-control-rooms/>

Newman, Lily Hay. "The Iran Hacks Cybersecurity Experts Feared May Be Here." *WIRED Magazine*. December 18, 2018. <https://www.wired.com/story/iran-hacks-nuclear-deal-shamoon-charming-kitten/>

"Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps." *U.S. Department of Justice*. March 23, 2018. <https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary>

Pagliery, Jose. "Iran Hacked an American Casino, U.S. Says." *CNN Business*. February 27, 2015. <https://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html>

Park, Donghui, Julia Summers and Michael Walstrom. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks." *The Henry M. Jackson School of International Studies, The University of Washington*. October 11, 2017. <https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>

Parsons, Ed and Michael Raff. "Understanding the Cyber Threat from Russia." *F-Secure Cyber Security*. Accessed November 10, 2019. <https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-russia>

Parsons, Ed and George Michael. "Understanding the Cyber Threat from Iran." *F-Secure Cyber Security*. Accessed November 10, 2019. <https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran>

Porche, Isaac. "Fighting and Winning the Undeclared Cyberwar." *RAND Corporation*. June 24, 2019. <https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html>

Porche, Isaac. "Getting Ready to Fight the Next (Cyber) War." *RAND Corporation*. March 3, 2018. <https://www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html>

Rumer, Eugene, and Richard Sokolsky. "Thirty Years of U.S. Policy Toward Russia: Can the Vicious Circle Be Broken?" *Carnegie Endowment for International Peace*. June 20, 2019. <https://carnegieendowment.org/2019/06/20/thirty-years-of-u.s.-policy-toward-russia-can-vicious-circle-be-broken-pub-79323>

"Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." *Cyber + Infrastructure, Department of Homeland Security*. March 15, 2018. <https://www.us-cert.gov/ncas/alerts/TA18-074A>

"Sandworm Team." *Mitre*. Accessed November 20, 2019. <https://attack.mitre.org/groups/G0034/>

Sanger, David. E. et al. "Chinese Army Unit is Seen as Tied to Hacking Against U.S." *The New York Times*. February 18, 2013. <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>

Sanger, David. E. and Nicole Perloth. "U.S. Escalates Online Attacks on Russia's Power Grid" *The New York Times*. June 15, 2019. <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>

Segal, Adam. *The Hacked World Order*. New York: PublicAffairs. 2016.

Sigholm, Johan. "Non-State Actors in Cyberspace Operations", *Journal of Military Studies* 4, 1 (November 23, 2016): 1-37, doi: <https://doi.org/10.1515/jms-2016-0184>

"Significant Cyber Incidents." *Center for Strategic and International Studies*. November, 2019. <https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

Spitzner, Lance. "Applying Security Awareness to the Cyber Kill Chain." *SANS Security Awareness*. May 31, 2019. <https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain>.

"The Cyber Kill Chain," *Lockheed Martin*, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

"The Global Risks Report 2019." *World Economic Forum*. January 15, 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

2016 Presidential Campaign Hacking Fast Facts." *CNN*. October 31, 2019. <https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html>

Uchill, Joe. "Iran's History of Hacking and Being Hacked." *Axios*. June 27, 2019. <https://www.axios.com/irans-history-of-hacking-and-being-hacked-ab1a9e96-63f1-4974-b75c-b72adc03dc51.html>

"U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage." *U.S. Department of Justice*. July 14, 2015. <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and>

"US-Iran relations: A brief history," *BBC News*, June 21, 2019 <https://www.bbc.com/news/world-middle-east-24316661>

Nakashima, Ellen, Greg Miller and Julie Tate. "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say." *The Washington Post*. June 19, 2012. https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

"U.S. Relations with China." *Council on Foreign Relations*. <https://www.cfr.org/timeline/us-relations-china>

Walls, Mike. "Nation-States: Why They Hack." *EdgeWave*. (April, 2015): 1-12. http://www.edgewave.com/wp-content/uploads/2015/04/EdgeWave_NationStates_WhyTheyHack.pdf

Walls, Mike. "Why Iran Hacks." *EdgeWave*, October 6, 2015. <https://www.edgewave.com/just-plain-interesting/dark-reading-exclusive-nations-hack-part-4-2/>.

“War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?” *The Economist*. July 1 2010. <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain>

“What is Economic Espionage?” *Federal Bureau of Investigation*. Accessed November 10, 2019. <https://www.fbi.gov/about/faqs/what-is-economic-espionage>

“What is a Zero Day Exploit?” *Kaspersky*. Accessed November 20, 2019. <https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit>

Wheeler, Tarah. “In Cyberwar, There are No Rules,” *Foreign Policy Magazine*, September 12, 2018, <https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/>

Wright, Thomas. “The Return to Great-Power Rivalry was Inevitable.” *Brookings Institute*. September 12, 2018. <https://www.brookings.edu/opinions/the-return-to-great-power-rivalry-was-inevitable/>

Yazid, N. M. “The Theory of Hegemonic Stability, Hegemonic Power and International Political Economic Stability.” *Global Journal of Political Science and Administration*: 3, no. 6 (2015):67-79.

Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.” *WIRED Magazine*. March 2, 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

Zetter, Kim. “The NSA Acknowledges What We All Feared: Iran Learns from US Cyberattacks.” *WIRED Magazine*. February 10, 2015. <https://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/>