INTERNATIONAL RELATIONS IN THE DIGITAL AGE:
GOVERNANCE AND SECURITY IN CYBERSPACE

A Thesis submitted to the faculty of
San Francisco State University
In partial fulfillment of
the requirements for
the Degree

Master of Arts

In

International Relations

by

Michael Roger Savvides

San Francisco, California

May 2020

Copyright by
Michael Roger Savvides
2020

CERTIFICATION OF APPROVAL

I certify that I have read *International Relations in the Digital Age: Governance and Security in Cyberspace* by Michael Roger Savvides, and that in my opinion this work meets the criteria for approving a thesis submitted in partial fulfillment of the requirement for the degree Master of Arts in International Relations at San Francisco State University.

See-Won Byun, Ph.D.
Professor

Anthony Pahnke, Ph.D.
Professor

Jonathon Whooley, Ph.D.
Lecturer

INTERNATIONAL RELATIONS IN THE DIGITAL AGE:
GOVERNANCE AND SECURITY IN CYBERSPACE

Michael Roger Savvides
San Francisco, California
2020

ABSTRACT The proliferation of Information and Communications Technologies is a gamechanger for international relations, and the classical theories are not suited for application in cyber studies. The current literature on cyber studies, is fragmented, and lacks a common theoretical framework. Additionally, the current cyber discourse treats cyber governance and cybersecurity as two separate concepts when in fact they are intertwined. This paper addresses these shortcomings by examining the models of cyber governance, followed by an analysis of key cybersecurity events. This paper takes a multi-disciplinary approach by synthesizing concepts from international law, computer sciences, and IR. After analysis of the preceding, this paper offers a novel theory, dubbed the Governance and Security in Cyberspace (GSC) framework, which is designed to understand IR as it relates to cyberspace.

I certify that the Abstract is a correct representation of the content of this thesis.

Chair, Thesis Committee

5/18/2020

Date

ACKNOWLEDGEMENTS

I would like to first thank the International Relations department at San Francisco State University for providing me the opportunity to pursue my academic goals. Thank you to Juanita Darling for working so hard to create the IR Scholars program. You made this journey possible in the first place. The members of this thesis committee have been particularly instrumental in the pursuit of this academic achievement; See-Won Byun, Anthony Pahnke, and Jonathon Whooley, without your instruction and guidance over the course of my academic career, this research would not have been possible.

Thank you to my family for your love and support. An incredibly special and loving thankyou to my wife Lisa, who inspires me to reach new heights. I could not have done any of this without you, thank you for seeing in me what I could not (also, I will now keep the desk neat and organized). Last and certainly not least, thank you to my son Caleb, whose very existence fuels my motivation each and every day.

TABLE OF CONTENTS

List of Table.....	viii
List of Figures.....	ix
Introduction.....	1
Defining Cyberspace and why study it in IR.....	4
Literature and Methodologies for understanding Cyber-governance	10
Review of Methodologies pertaining to cyber studies and IR theory.....	19
Research Design.....	20
Cyber Governance Models: The Multi-stakeholder Approach.....	27
Technical bodies: ICANN.....	29
Multinational Corporations: The power of connectivity	30
The State and International Law	36
The Multi-stakeholder model: What works and what does not	41
The State Sovereignty Model.....	42
China's internet and the Great Firewall	43
Russia and the RuNet.....	48
The State Sovereignty Model: What works and what does not	51

TABLE OF CONTENTS (CONTINUED)

Cyberwarfare and Cyber governance.....	53
Political tension meets cyberwarfare in Tallinn.....	53
The NSA and the Snowden Leaks	57
The PRISM Program.....	57
US-UK Partnership: Tempora.....	60
The Consequences of Prism and Tempora.....	62
Is IR theory applicable to cyber-relations?	62
Applying Realism and Liberalism to cyberspace	65
GCS Theoretical Framework	67
Assumptions, and actors in cyberspace	68
The Cyber International System	75
Power in cyberspace	80
Peace in cyberspace	83
Counter Argument	87
Conclusion	89

LIST OF TABLES

Table	Page
1. Realism and Liberalism key assumptions and prescriptions	26
2. Content Providers and their stake in international fiber-optic cable projects...	33
3. Topics and concepts discussed in the Tallinn Manual 2.0	39
4. Realism, liberalism assumptions versus GSC theoretical framework	68

LIST OF FIGURES

Figures	Page
1. Structure of research	25
2. Conceptualization of multi-stakeholder structure.....	28
3. Map of global undersea fiber-optic cables	32
4. Map of the Pacific Light Cable Network (PLCN)	35
5. China's active internet users in millions by year	46
6. Russian internet users as % of population, 1995-2018	49
7. NSA Introduction slide to the Prism program	58
8. Private sector actors and the data they collected via PRISM	60
9. International System proposed under GSC theoretical framework	76
10. Constitutional Order led by Predominant Power linked to others via informal ties	77
11. Origins of cyberwarfare attacks (excludes attacks of unknown origin)	84

The field of international relations (IR) was born out of political science in the mid-twentieth century and has its theoretical roots tying back to the ancient philosophers and Renaissance thinkers. IR seeks to explain the power dynamics between states on the international stage by applying various theoretical frameworks. These theories such as realism and liberalism, two of the oldest and most ubiquitous theories in IR, explain the world through lenses that were conceived before the age of the internet. So how do these theories apply now in explaining competing models of cyber governance? How do these theories contend with the notion of state sovereignty when the internet does not recognize borders on a map? Can today's IR help govern the internet, or does there need to be a new theoretical framework to govern cyberspace? Answers to these questions can be found across disciplines and this research will synthesize literature, concepts and processes found in international law, technical sciences, and international relations. This type of inter-disciplinary approach is necessary for new theorizing as well as to properly inform the course of policymakers and is the objective of this research.

The internet connects individuals, international organizations, multinational corporations as well as state agencies and governments, so how does this affect the international system? Another question this raises, is "are the traditional IR theories still relevant in the information age?". These are not simple questions and they require a deep understanding of current IR theories as well as an understanding of the agents and structures associated with societies connecting, communicating, conducting commerce and security in the realm of cyberspace. While there are certainly lessons to be drawn

from the traditional theories, I argue that the internet and Information and Communications Technologies (ICTs) have changed the landscape so irrevocably that these theories no longer serve their purpose and are essentially obsolete when dealing with cyber issues. This research will focus on the shortcomings of realism and liberalism because they are the two most common theories in the body of literature and testing them against cyber related issues is an important first step in developing a new theoretical framework (which will be presented later in this work) to analyze cyber relations and the international system.

IR scholars tend to view advancements in technology as independent variables rather than integral components of the state and international system, however, I contend that this view is incorrect and advancements in cyber technologies must be studied in their own right. I further argue, that due to the advent of cyber technologies, the international system has not seen this type of revolution since the development of nuclear technology; therefore, new theories need to be developed to make sense of this new landscape. International relations and cyberspace intersect at point which balances governance and security; these concepts are best demonstrated through competing methods of governance described in this research: (1) the multi-stakeholder approach (favored by the US); and (2) the 'state-sovereignty' approach (favored by the China-Russia cyber alliance).

While there have been a few attempts at analyzing the impact of the internet on the field of international relations there is still a significant amount of work to be done.

Cyber technologies connect every aspect of the international system from personal communication to military capabilities and therefore is a significant component to international relations which has been largely overlooked in the field. The advent of network connectivity and the subsequent cyber technologies are a ‘gamechanger’ for IR, on the basis of having created new vulnerabilities and altered international power structures.

In 1969, with the invention of the Advanced Research Projects Agency Network (ARPANET), technology made a significant leap, a leap with implications that would eventually affect every aspect of the modern world. The ARPANET, the internet’s precursor, “connected five sites: UCLA, Stanford, UC Santa Barbara, the University of Utah and BBN Technologies” which via computer “nodes” could transmit information packets via telephone lines (Bednarz, 2019). At the time, no one was aware that the world had begun a process that would eventually connect every corner of the globe. The ARPANET was developed by the US government’s Advanced Research Projects Agency (ARPA), an agency born out of the Cold War with the Soviet Union. After being caught off guard by Soviet advancements in nuclear and rocket technology, ARPA was formed to push the limits of science and technology in order to maintain supremacy over the Soviets (Lukasik, 2011).

It was in this post WWII / Cold War period that the field of International Relations came into modern existence and two theoretical camps emerged, realism and liberalism. Both are situated on fundamental assumptions about international actors, the

essence of power, and the organization of the international system. It is ironic that the internet (albeit in a nascent stage) and the development of these IR theories are approximately the same age but neither considers the other. The proliferation of ICTs have permeated every aspect of the international system and therefore affects every level of analysis, from the ‘individual’ all the way to the ‘system’.

While the study of cyberspace and cybersecurity has been around since the proliferation of computer technology in the mainstream (since the 1990s), it has mostly been undertaken by researchers in technological fields such as computer and information scientists. There is a small but growing body of scholarly research related to cyber issues in the field of IR but the research is fragmented and lacks a common theoretical framework. Following the current discourse on cyber issues in IR, my research will examine the current literature and their methodologies to synthesize what is currently written and build off that foundation. Before we examine the research other scholars have conducted, we must first understand the language; the next section will examine, adapt, and synthesize current definitions of key terms in the cyber discourse to help bridge the gap between the technical realm and IR theory.

Defining Cyberspace and why study it in IR?

Part of the challenge that IR scholars have in dealing with cyber issues is that it is commonly seen as a technological endeavor and that one must possess computer coding

and programming skills in order to study it. However, I contend that we in IR, are best suited to understand issues of cyber governance and policy making; this is because we study power and states relations, and cyberspace it is just a new arena to do so. In order to make the leap from states in the physical world to states in cyberspace we must understand a few key terms. This section of the literature review will focus on four key terms: Cyber-space, Cyber-conflict, Cyber-sovereignty, and Cyber-governance. This section will now present key definitions for critical terms from the emerging literature on cyber relations.

It is common to think of cyberspace as a virtual world, separate and autonomous from the physical “realm” but that idea overlooks the fact that anything “cyber” is rooted in the physical world via personal computers, servers, smart devices and even civil infrastructure. According to Shaji, Dev and Brindha, “cyber space is defined as an environment where storage, processing and communication are carried over computer and networking infrastructures” (2018, p. 3324). Shaji et al then connect the physical realm and the cyber realm with the term “Cyber Physical System”, this includes “applications in the areas of chemical processes, automotive, civil infrastructures, energy based distributors, aerospace, healthcare monitoring, entertainment, manufacturing, transportation, consumer appliances, military applications” (p. 3324). For the purposes of my research and theoretical framework, the term “Cyber-space” will include the aforementioned “Cyber Physical System” definition. In practice, the virtual realm and the physical cannot be separated in any discursive way, because if a physical system is

connected to the internet, it thus becomes a part of cyberspace. As an example, once an energy facility (physical realm) is connected to a digital network (virtual realm), it now also exists in cyberspace.

The next key term we must define is Cyber-conflict. This is a term that has many varying definitions in the current literature. In the same manner that some separate the physical realm from the cyber realm when discussing Cyber-space, so too do some scholars separate the two realms when defining Cyber-conflict. But since we cannot disconnect the cyber-realm from the physical, I adopt the definition put forth by Valeriano and Maness which defines, “cyber conflict as an aggressive foreign policy tactic in a developing domain that can also impact other arenas” (p. 348). These “other arenas” I define as including networks (lines of communication, personal computers, power grids) both civilian and government. I further define Cyber-conflict as being able to cause damage to not simply the cyber-realm, but also kinetic destruction in the physical world and the spread of misinformation.

Next we define the third key term, Cyber-sovereignty. When applying the term ‘sovereignty’ to states, we can look back to traditional IR theory to understand that this is a term that applies to a state that has control and orders its population and is clearly defined by a set of borders. The traditional and most commonly used definition of sovereignty originates from the Treaty of Westphalia; and as Pagallo states, the “Westphalian paradigm, such as the Leviathan’s monopoly on the legitimate use of force: wars to be declared by the competent authority of national sovereign states, so that such

authority can be held responsible for operations occurring in the course of the war” (p. 408). This definition simply does not translate to Cyber-space, a realm with no single population nor does it consist of any set of agreed upon borders. According to Yi, as interpreting international law based on the 1928 Island of Palmas ruling:

the sovereignty related with cyberspace is expressed as referent with the information infrastructures in a state’s territory, airspace, territorial waters and territorial sea; the direct consequence is that information infrastructures, regardless of their specific owners or users, are under the sovereignty of a country’s judicial and administrative jurisdiction, which is protected by sovereignty (p. 83).

Here again we see that the cyber realm and physical realm cannot be separated.

Finally, the final critical term is cyber- governance. For the purposes of this research, this is the most important term, not simply because it is the topic of this paper, but also because depending on the discipline of study, cyber-governance means completely different things. To better understand cyber-governance as a method, we need to first understand governance as a concept. Within the literature, there are varying definitions of governance, however most “involve some notion of collective steering” which can include such approaches as, “the price system; contracts; technical standards and system designs; governmental laws and regulations; norms and social conventions” (Mueller, 2017). Traditionally, and especially in IR, the state was viewed “as the ‘control centre [sic] of society’” but that top-down, hierarchical view has changed and the state is now “one actor among others” (Eeten & Mueller, 2012, p. 1410). I am not suggesting that the state is not important for governance, rather want to emphasis the fact that in an ever-

increasing globalized and connected world, the state is one actor among many that plays a role in transnational governance and especially in cyber governance. In international governance there are institutions and regimes which make rules and enforce norms which governs the behavior of actors on the international stage, however, cyber technologies have altered the landscape in such a way that international institutions are slow to adapt and few international regimes have been established over cyberspace.

The internet is a highly complex technical network of networks and as such, academics and professionals in the fields of technical communications, media and computer science focus their efforts on cyber-governance in terms of technical capabilities and frameworks. For example, there is a large body of literature dedicated to the study of the role that the Internet Corporation for Assigned Names and Numbers (ICANN) plays in the governance of the internet. However, the role of ICANN is grounded in the governance of internet domain names and primarily functions as a technical body. According to Christou and Simpson:

Internet expansion, particularly commercialization, meant domain names assumed increasing significance and value as global economic resources since they provide a recognizable presence on the Internet for those possessing them. Consequently, control over the system of the allocation and management of domain names became an issue of global political-economic significance from the mid-1990s. The result was the creation, in 1999, of a global organization, the Internet Corporation for Assigned Names and Numbers (ICANN), to address this issue (pp. 148-9).

The function of ICANN in governing internet domain names is the equivalent of the United States Post Office maintaining the system of addresses for physical locations in

the US. The role that ICANN plays in internet governance is critical and control of this system is at the heart of global internet governance. Whomever controls the domain name system (DNS) effectively controls whether the internet will remain open and free or fall subject to restrictions and closed networks. A more detailed examination of the role of ICANN and DNS will be discussed in a following section.

The academic research focusing on the role of ICANN in internet governance is important, however, it mostly deals with the technical architecture of the internet and fails to take a broader and more conceptual view of governance. When reviewing the literature on Internet governance, Eeten and Mueller note that those who, “use the Internet governance label typically do so in the context of discussions of the ICANN” (p. 726). For the purposes of this paper, I am utilizing the definition put forth by the United Nations at the 2005 World Summit on the Information Society, which defines Internet governance as, “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules decision making procedures, and programs that shape the evolution and use of the Internet” (United Nations, 2020). As I adopt this definition, I argue that it does not go quite far enough and should include cybersecurity and cyberwarfare as they affect states’ relations as well as the international system. Academic research as well as media and public interest has leaned heavily toward a discussion of cybersecurity, while governance has been left out of the public discourse. Internet governance and cybersecurity are commonly viewed as “alternative conceptual frames for understanding and guiding our approach to policy and

governance in a connected world” (Mueller, 2017, p. 416), however this paper argues that they are in fact related and intertwined concepts. No discussion about cyber governance should exclude the topic of cybersecurity and therefore the following paper will address this shortcoming of the current discourse.

Literature and Methodologies for understanding Cyber-governance

The study of ‘cyber’ is a broad and complicated field, that is why ‘cyber’ is the umbrella term and under that umbrella rests various specific fields of study. These fields include international law, technical fields (e.g. networks, computer science, communications), and international relations. Since the concept of ‘cyber’ is so broad, I will focus my research on global cyber-governance (how the various actors should interact with each other with in the cyber realm under an agreed upon set of rules, laws, and norms). In this research project, I will be synthesizing the three fields mentioned above into a theoretical framework more suited for international relations scholars to understand the significance of studying cyber-issues and applying it to case studies and policy making. The following articles reviewed pertain to cyber in one way or another but rather than focusing solely on their outcomes, I am also focusing on their methods for dissecting cyber related issues so that I may better formulate a method for my own research.

In their article, “The dynamics of cyber conflict between rival antagonists, 2001-11”, Valeriano and Maness create and test the theory that "restraint and regionalism

should be expected" as it relates to cyber conflicts. In order to test their theory, the authors use a data analysis (quantitative) methodology that compiles a dataset of cyber incidents and disputes for the timeframe listed above. Their dataset consists of 110 cyber incidents and 45 cyber disputes. In order to analyze the data, the authors identify key variables. The dependent variable (DV) is "cyber conflict" and the independent variables which affect the DV are types of cyber disputes: (1) nuisance, (2) defensive operation; (3) offensive strike; (4) nuisance and defensive; (5) nuisance and offensive; (6) defensive and offensive; (7) nuisance, defensive, and offensive. After analyzing their data, Valeriano and Maness conclude that "there is little evidence of cyber conflict in the modern era" (p. 357). Suffice to say, I take issue with their chosen methodology, and subsequent conclusion. The very nature of cyber conflict is subversive and secretive, even attributing a cyber-attack can be difficult if an attacker does not make their actions public. Specifically, I question how accurate the data set they compiled was and therefore their conclusions are incomplete and inaccurate. The authors anticipated this critique and stated that, "Some [cyber] operations will be hidden because they point to a specific weakness, but eventually the truth comes out. Many cyber operations committed in the last decade are public knowledge" (p. 351). Unfortunately, I cannot agree with that statement as there is no way to truly confirm whether or not their data set is complete or comprehensive enough to warrant such a definitive conclusion. This type of methodology could be very useful if only there was a centralized repository of cyber-conflicts that their data could be checked against but since there is not, the data may very well be drastically

incomplete; or alternatively, if there was a way to attribute an attack to an attacker as the next article will attempt to do.

The above article suffered from a crippling uncertainty in their data. So how to remedy this? A missing piece to their data is how to ultimately attribute a cyber-attack to a particular attacker? In other words, how does an actor know when they have been targeted and who is behind the attack? Lucie Kadlecova's article is an important work in advancing the understanding of attribution in the use of cyber warfare technologies. Given that attributing cyber-attacks can be extremely difficult, Kadlecova's article helps provide a foundation using qualitative 'indirect evidence' that can be used in other work to help attribute cyber-attacks. Attribution of cyber-attacks is a critical step in internet governance but because it can be difficult to identify a threat actor (as mentioned in the above critique of Valeriano and Maness), Kadlecova uses a case study analysis methodology to identify evidence for attribution. The author analyzes the Russian-Georgian armed conflict of 2008 and connects cyber activities, which he attributes to the Russian state, to the kinetic military operations on the physical battlefield. Through this case study analysis, Kadlecova identifies four independent variables: "(1) level of coordination; (2) level of preparedness; (3) state relations with the national hacker community; and (4) state conception of cyber-security" (p. 35). The author's variables and framework are solid points and through his case study of the Russian-Georgian armed conflict provides "international actors to attribute responsibility to states for attacks in cyberspace" (p. 42). However, as good as the methodology and framework are,

Kadlecova only tests these variables against a single case study, and furthermore, the use of “indirect evidence” hardly provides a state with legal justification for retaliation. This research could be useful for clandestine intelligence services but would not provide a strong foundation for scholarly academic research nor for policy makers. So what options are available to policy makers, governments or civil society? The next set of articles attempt to address the issue of “internet governance”.

In her interpretive study, Madeline Carr examines the 'multi-stakeholder' approach to Internet Governance and argues that it is the best method for governing cyberspace, and this model could renovate global governance as a whole. Furthermore, Carr argues that while there are many benefits to the multi-stakeholder approach, it "serves to reinforce existing power relations rather than disrupt them" (2015, p. 642). Methodologically, Carr employs a theoretical analysis of the "Gramscian approach to hegemonic power" (2015, p. 642). In order to qualitatively analyze her dependent variable (the multi-stakeholder approach), Carr identifies three groups of international actors, who also serve as her three independent components of the multi-stakeholder model: (1) the state; (2) the private sector; and (3) civil society. She contends that these three actors could offer the best option for power sharing in global internet governance with each group able to balance each other's interests, thus providing the most fair and equitable distribution of power. Given the fact that the internet was never designed to have a centralized structure (it is non-hierarchical by design), Carr's proposed multi-stakeholder approach does not seem too farfetched. However, this approach is not

without its problems and structural questions. When she identifies her independent variables, we must go beyond theory and question how each actor would share power in practice. Which states would participate? Which private sector companies would be allowed in? Are there any criteria for civil society groups or is any group allowed to take part? It seems like there would be an inherent bias towards the neoliberal democratic states and if that is the case then it is not a truly multi-stakeholder approach because it excludes certain states, companies, or societal groups. It could also be problematic among states in the global north vs global south who have different interests. I see some promise to this approach but also plenty of structural pitfalls.

In his 2015 article, Yi Shen utilizes a methodological approach that analyzes “historical and policy documents” to conduct a comparison of case studies between the United States’ and China’s policy of sovereignty in cyber-space. The author examines the concept of sovereignty in cyber-space as it relates to states (the United States and China in this case) and the each ‘state’s policy of cyber-sovereignty’: (1) cyber expansion; and (2) cyber defense. Yi Shen makes note of the importance of cyber sovereignty as it relates to security and international relations and takes an alternative approach to the previous authors when it comes to governance by stating, “though at the very beginning the term governance referred to governing without the government, the government, or the sovereignty state must be brought back in” (p. 83). He is not advocating against the multi-stakeholder approach we previously discussed but rather makes the case that the state should be the primary arbiter over sovereignty in cyberspace.

With that said, Yi identifies some asymmetries and inequalities among states in global cyber-space. He notes a difference in “resources and capabilities” among developed and developing states with regard to cyber capabilities, with the United States and European states as having a disproportionate advantage in capabilities and control over cyber infrastructure. His argument is that, as a result of the aforementioned ‘asymmetries’, US hegemony, in the physical and cyber realms, dictates that the US policy of cyber-sovereignty is one of cyber-offense while China’s policy is one of cyber-defense. He states that, “the US also makes clear proclaims of its “right to self-defense” to be used freely in cyberspace, which implies that the US has the right to attack the source of threat when the US considers itself under threat” (p. 86). China, on the other hand, Yi finds, is positioning itself in a more defensive stance because it is the weaker state; he says, “China will increasingly put special attention on ensuring sovereignty in cyberspace which is the main legal basement to ensure national security while China is the weaker side in the game of cyber security globally” (p. 91).

Yi’s article is an interesting case study analysis of two rival powers competing for dominance in cyberspace and raises questions about the role of states as unitary actors in that realm. This brings us full circle back to the question of how International Relations theory needs to be updated with cyber definitions, assumptions and prescriptions for states in cyber-space. The next three authors connect cyber studies with statecraft and IR theory.

As mentioned above, not nearly enough academic research is examining the relationship between technology and statecraft and IR theory; however, Madeline Carr, Professor of Global Politics and Cybersecurity at University College London (UCL) is among the leading academics in the field. She is among a small pool of scholars who are focused on “the ways in which new technology both reinforces and disrupts conventional frameworks for understanding International Relations and the implications of this for state and global security, order and governance” (University College London, 2019). In her 2016 book, *US Power and the Internet in International Relations: The Irony of the Information Age*, Carr argues that the current literature concerning information and communications technology (ICT) and international relations “has been done without adequately engaging with either technology theory or emerging and complex technical issues” (2016, p. 13). Carr further argues that the current literature is focused into two camps, the first views “ICT as simply an extension or enhancement of existing technology and therefore reinforcing existing power structures” (p. 3). The second camp she identifies in the literature, examines the relationship between “power” and “new technology as a transformative force” (p. 3), in other words, they view technology as an external factor on a state’s power rather than as a part of it. Carr does not dismiss the impact that technology has on states and state behavior but rather than examining it as an external factor, she views it as an integral component. In her book, she applies the “philosophy of technology” as a tool to bridge the gap between “new technology and state power” (p. 5). Ultimately, Carr views the current IR scholarship to be a starting

point in understanding the impact of technology on the international system, but it is not enough alone and must be informed by a new framework.

In his article, Lucas Kello makes the argument that cyber research should not only be left to the technologists but that the field is in need of "Scholarly study" and calls for a "congress of disciplines" to properly study cyber-studies as they relate to statecraft. Kello presents a theoretical analysis of cyber conflict and pursues three main arguments. (1) cyber studies integration into security studies is imperative for policy makers and "enhancing the field's intellectual progress" (p. 8); (2) the fact that cyber studies are technologically intricate, does not mean that scholarly work is impossible to conduct (you do not have to be a computer scientist to study cyber). (3) cyberweapons are not usually destructive in the "real world" and therefore do not fit into traditional conflict studies, this changes perceptions of warfare and international security. Kello makes a strong case for the need to study the "cyber issue" and acknowledges that the current literature is lacking. He warns against the "dangers of theoretical stagnation" by saying that "The implications of cyber activity for international anarchy and order, for example, have not been explored—even though practitioners repeatedly warn of global chaos. The conceptual apparatus of international security, in brief, is behind the times" (p. 13).

Methodologically, Kello employs a theoretical analysis of the three main schools of IR thought: (1) Realism; (2) Liberalism; and (3) Constructivism. By analyzing his three variables, Kello concludes that it may be possible to alter and adjust traditional IR theories and apply them to cyber studies but that it cannot be understated how significant

the “cyber revolution” is to state relations. He states that, “the cyber revolution is influencing the tendencies of anarchic international politics, rather than merely altering the strategic dealings of states; that is, the cyber domain exhibits both fundamental and instrumental forms of instability” (p. 39).

Kello’s theoretical analysis is a good foundation for my research into cyber governance and the relationship to IR theory. This article could serve as a bedrock from which to conceptualize a new theoretical framework, specifically tailored for the study of cyber issues in international relations. With that said, Kello’s article leaves something to be desired, he does not offer any solutions or theories but rather simply raises more questions and sounds the alarm for the need for more study. The next authors also present a theoretical analysis and further explain how to bridge the gap between theory and practice.

Johan Eriksson, and Giampiero Giacomello's article provides an important theoretical analysis between traditional IR theories and how they can or can not be applied to the "information revolution" (cyber studies). In a similar fashion as Lucas Kello did above, Eriksson and Giacomello take the three main IR “-isms” (three independent variables): (1) realism, (2) liberalism and (2) constructivism and extract their assumptions and analyze how they relate to cyber to possibly form a combination set of theories. The authors identify the most important aspects of cyber related issues to each theory. For realism, they tie the relevance of information warfare to security. For liberalism, they recognize the importance of security as well but add the multilateral

aspects and possibilities of cyber governance and that digital technology can be “a continuation and expansion of the trans-nationalization of society and economy” (p. 232). Lastly, the authors identify the significance of “social factors” in the constructivist school, specifically the “norms” that are created at the various levels of analysis (individual, state, international). Again, this methodological approach is significant in advancing the scholarly work pertaining to cyber studies in IR, but more than just presenting a theoretical analysis, Eriksson and Giacomello also advocate for the importance of translating this body of study into actual policy making. Eriksson and Giacomello conclude that while realism, liberalism and constructivism have served the field of IR well, a need “to develop middle-range theories that integrate” the 3 -ism is important in the digital age to properly inform policy, moving forward.

Review of Methodologies pertaining to cyber studies and IR theory

While cyber related research can seem out of the realm of IR, I argue that IR can provide an important bridge between theory and practice in cyber governance. Does the internet exist in a state of anarchy; and if so, how can states navigate the perils and pitfalls of an anarchical system without borders and treaties? Methodologically, cyber related studies will require a mixed methods approach, combining quantitative and qualitative methods, because as the previously reviewed scholars have demonstrated, this is a complex issue which must be examined holistically. My research will combine methods found in international law, communications as well as international relations. Empirical analysis will be required to form a foundation from which to theorize about the

various possibilities for cyber governance structures. This will include further study of the “multi-stakeholder” approach as well as the state centric approach. Cyber related studies are relatively new, and much work needs to be done so that as societies integrate these technologies into our daily lives, scholarly work can provide guidance to policy makers.

Research Design

This research will examine the utility of the two most prevalent theories utilized in the field of International Relations, realism, and liberalism, as they relate to cyber technologies. The two theories operate under assumptions about the global system, based on the world at the time they were created, however, the world system has been altered by the introduction of the internet. Fiber-optic cables stretch across the globe and under the seas to connect communities, economies, and states. The internet is a network of networks that is connected by these cables and cross over borders with few controls or checks. It has changed how societies communicate, economies function, states govern, and warfare is conducted, so it stands to reason that research into how traditional IR theories hold up to the changing landscape is warranted.

From within the sources in the literature review, I have identified two distinct approaches to cyber governance. The first, the method that the United States and its political and economic partners utilize, is the ‘multi-stakeholder’ approach which incorporates actors from the public and private sectors as well as civil society. The second is what is referred to as, the ‘state-sovereignty’ approach, and this is method is

utilized by the People's Republic of China and the Russian Federation, is characterized by defensive measures such as the use of government-controlled networks, surveillance and firewalls.

What is the best method to answer the question of relevance of IR theory in the digital age? Quantitative data for analyzing attacks would be largely flawed given that accurate data would be difficult to attain. Cyber-attacks, especially those conducted by states or attacks that target states are not often made public. Reports from private security firms are not subject to peer review and their collection methodologies are not a matter of public knowledge and so any data sets provided by these companies are questionable. Quantitative research, at least at this point, would not provide an accurate assessment and would have to be caveated, thus making it less than ideal.

Much of cyber related issues are, by design, kept confidential and away from public scrutiny. Given the secretive nature of states' cyber operations and structures, quantitative analysis is not particularly suited for research on this topic. However, given the understudied relationship between theory and cyber governance, qualitative methods could be better suited for analysis in this regard. Andrew Moravcsik writes that, "Qualitative analysis is ... unmatched in its flexibility and applicability: a textual record exists for almost every major international event in modern world history "(Moravcsik, 2014, p. 663). So, what types of data can be utilized to conduct an analysis of cyber governance? Much of the existing literature on cyber governance is theoretical in nature and there are some attempts to synthesize international law, cyber technologies as well as

IR theory (Kadlecova, 2018) (Pagallo, 2015) (Yi, 2016), but few have attempted to examine the relevance of IR theory in the digital age and determine its prescriptive and predictive powers, and no one to my knowledge has attempted to formulate an original cyber-based theoretical framework for application in the field of international relations.

In order to prove that realism and liberalism are not properly equipped for cyber related issues in IR, a case study analysis will follow; one that will select deviant cases, “whose outcomes do not fit ... prior theoretical expectations” (Bennett & Elman, 2007, p. 176). After analyzing the multi-stakeholder and state sovereignty models of government, I will examine two significant case studies: (1) the first documented cyberwar which target the state of Estonia in 2007; and (2) the case of the National Security Agency’s Snowden leaks in 2010. I argue that these cases are deviant, in that they prove a deviation from the expected outcomes, based on traditional IR theory. Deviant cases, rather than typical cases, are best suited for discovering previously overlooked or ignored outcomes (Seawright, 2016). Therefore, analysis of deviant cases provides the best opportunity to introduce a new theoretical framework, specifically tailored to the relationship between IR and cyber. By prioritizing and selecting deviant cases for this study, this research will show the need for an updated theoretical framework, through which cyber-issues and international relations can be best understood.

The following will identify the agents and structures for each model of internet governance as well as cybersecurity. This research will identify and examine the role of relevant actors in cyber-governance and cybersecurity. Beginning with the multi-

stakeholder model of cyber governance, the actors are a combination of public, private, and civil society groups. They include: (1) technical bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN); (2) Multinational corporations, mainly internet content providers, like Google and Facebook, and telecom giants, like ATT and Verizon; and finally (3) state level governments. These three spheres comprise the multi-stakeholder model to cyber governance. Each provides a specific function within the model and are represented together as a model of checks and balances, ensuring a fair and equitable management system for the governance of the internet for all those who participate in this model.

Secondly, the cyber sovereignty model of governance has fewer actors and a more centralized structure. Within this model, states are the primary actors and are accompanied by their respective “technology champions”. The two most notable states who adhere to the state sovereignty model are the Russian Federations and the Peoples Republic of China. States such as China and Russia, feel that the US is continuing their hegemonic ambitions into cyberspace. As a result, China and Russia have become increasingly active in international discussions concerning cyber governance policy and promoted the notion of “Cyber Sovereignty” (also sometimes referred to as Internet Sovereignty, or State Sovereignty model) as a method of cyber governance. They are technologically advanced, thanks in part to their tech champions. Yandex and Baidu are Russia and China’s tech champions respectively, and are direct competitors to the US’

Google Corporation (Budnitsky & Jia, 2018). The tech champions based in these states, where power is centralized, work closely with the state to achieve state goals.

When examining cybersecurity, I will focus on two specific cyber-related events. These events, I have determined are two of the most significant with implications that have had long lasting impacts on cyber security and governance. The first, are the series of systematic cyber-attacks which targeted the state of Estonia in 2007 and persisted for three weeks. During this period, the state's cyber-infrastructure was targeted and crippled the government's ability to function. This series of events, shows the significance of high-level and low-level cyber-attacks through the first known case of a sovereign state being the target of cyberwarfare.

The second cybersecurity event I will examine, are the operations conducted by the NSA, revealed by the top-secret leaks of Edward Snowden. The former government contractor illegally removed approximately 1.5 million files and leaked a portion to the media. There are several revelations in these documents, but the two that I will argue that have some of the most significant relevance to my research are: (1) The details behind the NSA's PRISM program, and (2) the United Kingdom's GCHQ 'tapping' of undersea fiber-optic internet cables. These two operations demonstrate that realism and liberalism cannot adequately prescribe policy or predict events in the digital age and will be discussed in detail in a following section. These two events as well as the discussion to come concerning the multi-stakeholder and state-sovereignty models, will serve as

deviant cases which prove the necessity for a new IR theory, specifically designed to understand the world system through a cyber lens (see figure 1).

Figure 1: Structure of research

Following this research design, my analysis will begin with understanding the agents, structures and processes involved in the previously mentioned cyber governance models and cybersecurity events. After which, an examination of realism and liberalism will ensue to determine if and how their key assumptions translate to the case study findings. Any deficiencies in their theoretical framework will be addressed in my original theory, presented in the last section of this research.

Realism and liberalism, just like any other IR theory, view the world through a specific lens which is built upon certain theoretical assumptions (see table 1). Take for example, realism which views the world through a pessimistic lens where states are the only meaningful actors, are only concerned with their own self-interests and peace is achieved through predominantly military might. The emphasis on military and economic power (hard power) capabilities is prevalent in realist literature. However, hard power

does not necessarily translate to cyber topics. Realism's view of power is built upon military capabilities and the use of those capabilities to inflict kinetic destruction and/or severe loss of life. Cyber capabilities alter this line of thought. While there is currently only one known case of cyberwarfare which directly achieved kinetic damage in the physical realm (STUXNET attack on Iran revealed in 2010), the majority of cyber-attacks disrupt communications, spread misinformation, and disable critical infrastructure.

Table 1: Realism and Liberalism key assumptions and prescriptions

Views	Realism	Liberalism
Human Nature	Pessimistic: Hobbesian principles	Optimistic: Kantian principles
Key actors	States (top-down)	States, IGOs (top-down)
International system	Anarchical	Anarchical, but growing world order
Main cause of conflict	States are self-interested	No central authority to regulate competition
Power preference	Projecting and using hard power	Encourage interdependence & cooperation, prefer soft power (attracting others w/o coercion)
Best path to peace	Hegemon establishes order (zero-sum)	Interdependence maintains peace (zero-sum)

Cyber-attacks are not considered seriously by realism and are dismissed as minor offenses (Rid, 2012). Rooted in the realist tradition, Erik Gartzke contends that “Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless

they can impose substantial, durable harm on an adversary... this will occur only if cyberwar is accompanied by terrestrial military force” (Gartzke, 2013, p. 43). At most, realism views cyber war as an element of traditional warfare and as such, fails to understand the implications and changing dynamics between rival and emerging powers.

The following research will present qualitative evidence that proves cyber technologies are indeed gamechangers in the field of international relations and that the traditional paradigms of realism and liberalism do not fully understand this shift. After an analysis of deviant cases, I will present an original theoretical framework, designed specifically for understanding international relations in cyber-space. This original theoretical framework will explain how a cyber lens differs from realism and liberalism with regards to foundational principles and key assumptions about the world system. These points will diverge from the Hobbesian/Kantian views of human nature, and explain who the relevant actors are, what structure does the international system take, what are the causes of conflict, power preferences and prescription for a path to peace.

Cyber Governance Models: The Multi-stakeholder Approach

As previously discussed, the multi-stakeholder approach is a collaboration between the state, private sector actors, and civil society (Carr, 2015). This approach to cyber governance is the dominant model and was pioneered by the United States, along with their allies in Europe and has been adopted by most developed liberal democracies (Carr, 2015). This model is comprised of three groups of actors; however, it becomes much more complex as we begin to examine actors within each group of actors. The

multi-stakeholder model is a collection of “norms, institutions and procedures” (Nye, 2014, p. 7) and this portion of the paper will examine key actors of the multi-stakeholder model and their roles. As mentioned previously, the actors and procedures involved in this model of cyber governance span various fields, from state agencies and technical bodies to multinational corporations and non-governmental organizations. The complexity of this model is illustrated in figure 2. The following section will dissect and simplify the interconnected relationships that actors from each sphere engage in with regards to cyber governance.

Figure 2: Conceptualization of multi-stakeholder structure

Source: Nye 2014

Technical bodies: ICANN

At the center of the diagram is the previously discussed ICANN which “helps coordinate the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet’s underlying address book, the Domain Name System (DNS)”;

put simply, “ICANN defines policies for how the ‘names and numbers’ of the Internet should run” (Internet Corporation for Assigned Names and Numbers, 2020). This is a critical function of the internet and without an international standard like the one ICANN presides over, the internet could not function properly. The operations of ICANN, from its beginning in 1998, has always been operated as a non-profit but were originally under the oversight of the US Commerce Department, and the government contract with ICANN expired on September 30th, 2016, at which time the US government did not attempt to renew the contract and ICANN became a fully independent organization with no government oversight (Sydell, 2016). It is at this point that the makings of the multi-stakeholder approach begin to take true form. Critics of American withdrawal from control of ICANN functions claimed that authoritarian governments would seize control of the internet.

One of the most vocal critics was American Senator Ted Cruz who said: “Russia, and China, and Iran don’t have a First Amendment... they don’t protect free speech, and they actively censor the Internet. ICANN could do the same thing, putting foreign countries in charge of what you can say online, prohibiting speech that they disagree with” (Sydell). So far, Cruz’s predictions have not come true, and ICANN’s board of directors is comprised of a multi-sector, global array of actors, which include, and have

included former business executives, nonprofit leaders, policy analysts, legal analyst and academics. While ICANN is now independent of the US government, it is still an American based corporation and as such the US government has legal jurisdiction over the nonprofit. According to their website:

“Externally, ICANN is an organisation incorporated under the law of the State of California in the United States. That means ICANN must abide by the laws of the United States and can be called to account by the judicial system i.e. ICANN can be taken to court. ICANN is also a non-profit public benefit corporation and its directors are legally responsible for upholding their duties under corporation law” (Internet Corporation for Assigned Names and Numbers, 2020).

So, while it is true that ICANN is an independent organization, it is not free from American influence or legal action, meaning that Cruz’s earlier warnings are ultimately unfounded. If ICANN were to begin censoring the internet or allowing an authoritarian takeover of the internet, the US government and even civil society groups would have the ability to challenge their behavior in court with a high chance of success.

Multinational Corporations: The power of connectivity

In the multi-stakeholder model, multinational corporations play a significant role in not just governance of the internet, but the very physical structures which allow the internet to function. For this section, I have chosen to examine the role that telecommunications companies, internet service providers (ISPs), and other internet technology companies play in the governance model depicted in Figure 2. The

overwhelming majority of global internet traffic passes travels via fiber-optic cables that connect countries all around the globe.

While most people understand the internet as being wireless through mobile phones or Wi-Fi capable devices, the information they send and receive is eventually transmitted via fiber-optic cables. Furthermore, if the data is stored overseas, that data travels across cables that span oceans. Globally, 99 percent of all internet data transmitted is carried by this network of undersea cables (Starosielski, 2015). The global network of submarine cables consists of 406 individual cables, which if combined, are just over 745,645 miles in length (see figure 3) (TeleGeography, 2020). Undersea fiber-optic cables were first deployed by telecom companies in the late 1990s who then sold the bandwidth to consumers. Some of the most famous of these telecom companies who own and operate these cables are AT&T and Verizon. While the original network of undersea cables still operates today, new cable projects are being funded by non-telecom companies such as Microsoft, Amazon, Google and Facebook (Satariano, 2019). These telecom companies and internet titans are responsible for the physical cables which the internet is comprised of. Recall that the previously discussed ICANN serves as a steward of the internet's address book, so extending this analogy, Microsoft, Amazon, Google, AT&T (and many others) are the keepers of the roads and highways that international internet traffic flows through.

Figure 3: Map of global undersea fiber-optic cables

Source: TeleGeography 2020

As keepers, of this vast network of cables, major corporations, based in countries all around the world are responsible for maintenance, repairs and overall reliability. This is an incredibly important function which everyone depends on. The responsibility of these cable lines is truly interdependent “because no single actor has ownership over the entire network: cable routes are shared between consortiums of companies; its jurisdiction falls under both national and international laws; and coordination between companies and countries is necessary to ensure speedy repairs when outages occur” (Ross, 2014, p. 143). With so much responsibility, these consortiums play a significant role in the multi-stakeholder model. Within this power structure, content providers and

social media companies are becoming increasingly invested in undersea fiber optic cables (see table 2).

Table 2: Content Providers and their stake in international fiber-optic cable projects

Content Provider	Fiber-Optic Cable	Ownership Stake	Countries Connected
Google	FASTER	Part Owner	USA, Japan, Taiwan
	Junior	Sole Owner	Brazil (Domestic)
	Monet	Part Owner	USA, Brazil
	Pacific Light Cable Network (PLCN)	Part Owner	USA, Philippines, Taiwan, China
	Southeast Asia Japan Cable (SJC)	Part Owner	Japan, China, Hong Kong (China), Philippines, Brunei, Singapore
	Tannat	Part Owner	Argentina, Uruguay, Brazil
Facebook	Asia Pacific Gateway (APG)	Part Owner	S. Korea, China, Vietnam, Malaysia, Japan, Thailand, Singapore, Taiwan
	MAREA	Part Owner	USA, Spain
	Pacific Light Cable Network (PLCN)	Part Owner	USA, Philippines, Taiwan, China
Microsoft	AEConnect	Major Capacity Purchaser	USA, Ireland
	Hibernia Express (GTT Atlantic)	Major Capacity Purchaser	USA, Canada, Ireland, UK
	New Cross Pacific (NCP) Cable System	Part Owner	USA, S. Korea, China, Japan, Taiwan
	MAREA	Part Owner	USA, Spain
Amazon	Hawaiki	Major Capacity Purchaser	USA, Australia, New Zealand

Source: TeleGeography 2020

Given that Google and Facebook are the two largest actors among content providers who are investing in undersea fiber optic cable lines, and they have combined their efforts and resources into the joint cable named the Pacific Light Cable Network

(PLCN), a deeper dive into their vertical integration into this space is warranted. Google and Facebook are primarily content providers, which means they provide digital platforms and services for individuals, companies, and even governments. As a means of diversifying, both companies have adopted a vertical integration strategy by expanding into fiber optics lines, so now, they do not just own the platforms and services, but also the lines through which the internet traffic flows.

The PLCN was first announced in 2017 and “was touted as the first subsea cable directly connecting Hong Kong and the United States, allowing Google and Facebook to connect speedily and securely with data centers in Asia and unlock new markets” (Harris, 2020). The cable was built with five landing points: (1) El Segundo, California; (2) Baler, Philippines; (3) San Fernando City, Philippines; (4) Toucheng, Taiwan; and (5) Deep Water Bay, Hong Kong, China (see figure 4). The project has been completed, however, because these cable lines are the backbone of connectivity worldwide, the US government has oversight of these types of projects (when a US based company is involved and at least one landing point is located on US soil), and the PLCN is still waiting on regulatory approval. A group “of representatives from the U.S. Department of Homeland Security, the U.S. Department of Justice and the U.S. Department of Defense” who are referred to as “Team Telecom” are responsible for “risk assessment, mitigation and oversight” (Brown, Daly, & Moss, 2018), and they have stalled the complete opening of the PLCN.

Figure 4: Map of the Pacific Light Cable Network (PLCN)

Source: TeleGeography 2020

Team Telecom’s apprehension to greenlight this project comes from the fact that the PLCN is partially backed by a Chinese company, Dr Peng Telecom & Media Group, which is not a Chinese state-owned entity but has worked closely with Huawei, who the US government has long been suspicious about. Google and Facebook grew tired of waiting for approval to link the US and Hong Kong, and since Team Telecom’s issues reside with possible Chinese government involvement, the tech companies filled a “Special Temporary Authority” (STA) with the Federal Communications Commission (FCC) requesting “to operate limited portions of the Pacific Light Cable Network” (Request for Special Temporary Authority, 2020). To get the PLCN operational, Google and Facebook have proposed authorization for activating the lines connecting landing points in the US, Philippines, and Taiwan; and for the time being, leaving the connection

to Honk Kong inactive. Google (referred to as GU Holdings in the STA filed) and Facebook (referred to as Edge USA in the STA) argued to the FCC that:

“Segments S1.1.1, S.1.1.2, and S.2 (connecting the United States to Taiwan) are now fully constructed, tested, and ready for commercial operation. As explained below, GU Holdings and its affiliates urgently need the capacity of those segments to support their internal operations and this STA would serve the public interest. Edge USA expects that Segments S1.2 and S3 (connecting Baler, Philippines, with Branching Unit 1, with onward connectivity to the United States on Segments S1.1.1 and S1.1.2), the capacity of which will also serve the public interest ... Grant of the requested STA will serve the public interest, convenience, and necessity and otherwise comply with U S law and Commission regulations. Indeed, without access to PLCN’s U S Taiwan capacity, the value of large, recent capital investments Google has made in the United States is significantly reduced” (Request for Special Temporary Authority, 2020, pp. 4, 6).

At the time of this writing, Google and Facebook are awaiting a decision from Team Telecom, but this highlights a key component of the multi-stakeholder model, all the actors are interconnected and even with Google and Facebook’s considerable wealth, power and influence, they are still dependent on approval from the state.

The State and International Law

The PLCN is a good case study of the relationship between two levels of actors found within the multi-stakeholder model, corporations, and governments. At the state-level of analysis, governments wield a great deal of power but are still not able to act unilaterally in creating and implementing policy and governance standards. While it is true that each state decides what “cyber policies” it will enact, what international internet projects it will allow (e.g. the Google, Facebook PLCN cable), at a domestic level, the

international community is far behind in establishing laws, norms and regulations across all areas of interest. At the international level, the community has been slow to address cyber related issues and “it took until 2013 for state representatives to agree that international law even applies to cyberspace” (Mačák, 2017, p. 879)

As a framework for establishing consensus on cyber governance, international law serves as an obvious starting point for states, international organizations, civil society and any other stakeholders. Questions around state sovereignty and international law have been sticking points for agreement and cohesion when dealing with cyber issues at the international level. States seem reluctant to directly address specific issues related to cyber relations in legal terms, and instead have favored agreement of norms rather than legally binding rules which “gives rise to international legal responsibility” (Mačák, p. 882). However, even with efforts concentrated on establishing norms, rather than laws, states have been reluctant to commit themselves. In its most recent substantive report, members of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications (UN GGE), made “recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behavior of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment” (UN GGE, 2015, p. 7). While the report from the UN GGE made recommendations on a “voluntary, non-binding” level, two of the contributing members of the report, the US and China, “refrained from committing themselves to any of the proposed norms” (Mačák, p. 882).

Within the multi-stake holder model, almost everyone who is committed to a “free and open internet” can contribute their opinions and attend various conferences and summits, all of which aim to influence policy makers. However, this often leads to fractious results and leaves more divergent opinions on what the course that internet governance should take. In an attempt to provide all stakeholders with a common legal framework, the NATO Cooperative Cyber Defense Center of Excellence (NATO CCDCOE) was initiated on May 14 2008 and was “award[ed] full accreditation and International Military Organization status... the same year in October” (CCDCOE, 2020).

One of the CCDCOE’s first major achievements was the organization of the Tallinn Manual process in 2009, which “invited an independent group of experts to produce a manual on the international law governing cyberwarfare”, but recognizing that cyber issues extend beyond warfare, NATO “expand[ed] the Manual’s scope to include the public international law governing cyber operations during peacetime” (Schmitt, 2017, p. 1). The need for such a document was in response to escalating malicious cyber activities that targeted state level actors, such as the cyber-attacks on Estonia in 2007 and on Georgia in 2008 (further discussion on cyber-attacks in a following section) (Schmitt, 2013, pp. 1-2). The first version of the Tallinn Manual was published in 2013 and the most updated Tallinn Manual 2.0 was published in 2017, which included the contents of version 1.0 but expanded into “legal analysis of more common cyber incidents that states encounter on a day-today basis that fall below the thresholds of the use of force or armed

conflict” (CCDCOE, 2020). The Tallinn Manual 2.0 methodologically and systematically outlines legal interpretations of critical terms and concepts that apply to cyberspace (see table 3), but as it relates to this paper, among the most crucial, is the clarification of state sovereignty in cyberspace.

Table 3: Topics and concepts discussed in the Tallinn Manual 2.0

General international law and cyberspace

- Sovereignty
- Due Dilligence
- Jurisdiction
- International responsibility
- Cyber operations

Specialised regimes of international law and cyberspace

- International human rights law
- Diplomatic and consular law
- Law of the sea
- Air Law
- Space Law
- International telecommunication law

Interntional peace and security and cyber activities

- peaceful settlement
- prohibition of intervention
- The use of force
- Collective security

The law of cyber armed conflict

- the law of armed conflict
- Conduct of hostilities
- Certain persons, objects and activities
- Occupation
- Neutrality

Source: Tallinn Manual 2013

The International Group of Experts applied the concept of sovereignty in cyberspace as follows:

For the purposes of this Manual, the physical, logical, and social layers of cyberspace are encompassed in the principle of sovereignty. The physical layer comprises the physical network components (i.e., hardware and other infrastructure, such as cables, routers, servers, and computers). The logical layer consists of the connections that exist between network devices. It includes applications, data, and protocols that allow the exchange of data across the physical layer. The social layer encompasses individuals and groups engaged in cyber activities (2017, p. 11).

The experts then express their opinion that while the referencing of cyberspace as “a ‘global domain’ or ‘fifth dimension’” can be appropriate for some discourses, in terms of international law they are not accurate. This is because by designating cyberspace as being a ‘virtual’ space, it ignores the fact that all the components of the internet existing in physical form and reside somewhere within a territorial space (2017, pp. 11-12).

Many historians and political scholars understand the concept of state sovereignty as being a product of the Peace of Westphalia in 1648 and applied as law directly to the international system among states. However, sovereignty was not “historically constructed and then applied, sovereignty emerges as an historical fact that was gradually recognized by statesmen and eventually acknowledged as reality” (Croxtton, 1999, p. 571). Furthermore, the concept of sovereignty has been shaped by how states want the rule to apply; “with respect to espionage, states have not found espionage to be a per se violation of sovereignty, even when those actions take place in and/ or have effects in another state”, and states “support the assertion that sovereignty is a principle that gets applied based on the practical imperatives of states, rather than as a uniform rule of international law” (Jensen, 2017, p. 742). The same historical path may be true of sovereignty as it applies to states and cyberspace. With little consensus among states on

agreeing to legally binding rules today, it may be some time before a clear-cut definition of how sovereignty applies to cyberspace emerges.

While the Tallinn Manual is widely referenced in cyber related discourse, it is important to note that the Manual is simply an interpretation of international law as it might be applied to cyber issues on the international stage. Furthermore, the Tallinn Manual is not a legally recognized document; the Manual itself reads:

It is essential to understand that Tallinn Manual 2.0 is not an official document, but rather the product of two separate endeavors undertaken by groups of independent experts acting solely in their personal capacity. The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. Nor does it reflect the position of any other organisation [sic] or State represented by observers or of any of the States involved in the ‘Hague Process’, which is described below. Finally, participation as members of the International Group of Experts or as peer reviewers by individuals who hold governmental positions in their respective countries must not be interpreted as indicating that the Manual echoes the viewpoints of those countries (p. 2).

Even though the Tallinn Manual is not a legal document, it does provide all stakeholders with an interpretation of existing international law with the appropriate language as it relates to cyber activities, and it could serve as the necessary foundation for future cyber treaties and establishment of norms and laws.

The Multi-stakeholder model: What works and what does not

If we observe the multi-stakeholder model as a three-tier hierarchical diagram, with technical bodies at the bottom (e.g. ICANN), corporations in the middle (e.g. telecoms and content providers), and states and IOs at the top (e.g. US, China, NATO,

UN), there seems to be less agreement and cohesion in the multi-stakeholder model the higher up the chain we go. At the base level, technical agreement (ICANN) is not widely disagreed on, at the corporate level, private enterprise seems more than willing to take on the risks and responsibilities of creating and maintain cyber infrastructure, at the international level, the legal implications of international law versus norms seems to be stalling cohesion among states.

While there are some potential conflicts with the multi-stakeholder model of internet governance, it presents some promising aspects, for example, the fact that there are several actors who must find common ground and mutual understandings. This type of cooperation lends itself to utilization by allied and ‘like-minded’ states. As previously mentioned, the internet is a network comprised of other networks, it has always been a non-hierarchical structure without a centralized power structure and therefore, the multi-stakeholder model fits in with this structure, and ideally, should promote ‘power sharing’ among its various actors.

The State Sovereignty Model

While most states are participants (to varying degrees) of the multi-stakeholder model, there are some states who feel that the United States and its European allies have too much sway in determining cyber governance policy. States such as China and Russia, feel that the United States are continuing their hegemonic ambitions into cyberspace. As a result, China and Russia have become increasingly active in international discussions

concerning cyber governance policy and promoted the notion of “Cyber Sovereignty” (also sometimes referred to as Internet Sovereignty, or State Sovereignty model) as a method of cyber governance.

China’s internet and the Great Firewall

At the 2015 World Internet Conference in Wuzhen, China, President Xi Jinping delivered the keynote speech in which he said:

China is going through a historic process of rapid application of information technologies. China attaches great importance to Internet development. Since China was connected to World Wide Web 21 years ago, we have, in keeping with the principles of proactive utilization, rational development, law-based regulation and assurance of security, strengthened IT infrastructure, developed cyber economy and made life better for our people through IT application. In the meantime, we have conducted governance of cyberspace in accordance with law and ensured a clean environment in the cyberspace. Today, China is already home to 670 million Internet users and over 4.13 million websites. The Internet is now deeply integrated into China's economic and social development and the life of the Chinese people. The principle of sovereign equality enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations. It covers all aspects of state-to-state relations, which also includes cyberspace. We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security (Xi, 2015).

Rather than conform to a global standard of internet governance, China would rather govern their portion of the internet as they see fit, without outside interference and China’s method of governance over their portion of the internet is based on censorship

and the monitoring of activities. In February of 2014, China's Central Committee appointed Xi "as head of the Central Leading Group for Cyberspace Affairs" (IT Advisory KPMG China, 2017, p. 4) and the beginnings of heightened focus on cyber security and affairs had begun. The 2015 speech was an announcement to the world that cyber affairs would be of central importance to China. By November of 2016, China passed the Cybersecurity Law of the People's Republic of China, which aimed to solidify domestic control over information systems and regulate how foreign corporations are allowed to handle data domestically (IT Advisory KPMG China).

The term Internet Sovereignty began to gain traction in political discourse after a 2010 white paper was published by the Information Office of the State Council of the People's Republic of China. The 14-page document discusses the importance of the internet as it relates to China's continued development efforts and argues that the policies that China chooses to implement within its borders should not be a concern for external actors. The white paper specifically lays out that, "laws and regulations clearly prohibit the spread of information that contains contents subverting state power, undermining national unity, infringing upon national honor and interests" (White Paper - The Internet in China, p. 5). This had been policy of the Chinese Communist Party (CCP) since they came to power but have applied the same laws and regulations to internet traffic within their borders, and in what seems to be a direct message to the 'West', the white paper states that, "Within Chinese territory the Internet is under the jurisdiction of Chinese

sovereignty. The Internet sovereignty of China should be respected and protected” (p. 11).

The CCP was not always this strict when it came to internet governance. In 1987, the first email originating in China and sent across its borders was sent by a pair of computer scientists to their partners in Germany. The email was sent via an “email node”, similar to the system used by the creators of the ARPANET decades earlier; the email header said, “Across the Great Wall we can reach every corner of the world”. By 1994, “scientists from the Institute of High Energy Physics at China’s Academy of Sciences built the first cable connection to the World Wide Web” in partnership with scientists at Stanford University and with that connection China began to integrate into cyberspace (FlorCruz & Seu, 2014). At first, China embraced the use of ICTs and internet cafes became popular in large cities. Citizens were able to connect to the internet without restrictions and Chinese academics were connected to their peers across the globe. China was embracing the principles of an open and free internet, that is until the CCP realized that the internet gave too much freedom to non-Party actors; as a result, the government began development of China’s Golden Shield Project, more commonly known as China’s ‘great firewall’ and began widespread operation in 1998.

Also, in 1998, an emerging political party began to form, and grew its outreach and standing using the internet. The Chinese Democratic Party (CDP) was a group that was “skilled in modern communication techniques” and “called for multiparty democracy in China” as well as “respect for human rights” (Human Rights Watch, 2000). The CCP

utilized the Golden Shield project to block CDP websites and internet traffic as they were viewed as subversive group and threatened the stability of the party and undermined social cohesion under the CCP.

When the term ‘China’s great firewall’ is used in the media, it invokes an idea that all internet traffic is blocked from the outside and that, domestically, China operates its own network. The truth is that China is as connected to the internet as most other countries, except that China’s great firewall works to monitor internet traffic, and censors content which the state deems to be in violation of CCP laws and regulations. Controlling internet traffic in a country with over 900 million active internet users (see figure 5) is no small feat and for the great firewall to be effective, it uses a multitude of techniques.

Figure 5: China’s active internet users in millions by year

Source: Statista 2020

China's great firewall uses techniques such as blocking IP addresses, filtering URLs, deep packet inspections, resetting connections between users and servers, and blocking virtual private networks (VPNs); these are just some of the technical methods utilized and much of it is automated using sophisticated algorithms and artificial intelligence. Beyond the automated computer systems used to control the internet within its borders, China also uses human monitors. A newspaper article, published in the state-owned *Beijing News*, outlined the government's position for an "Internet public opinion analyst". The article explains a further expansion of human assets used for internet monitoring and the recognition as an official government occupation:

"the public opinion monitoring room of People's Network will hold the first public opinion analyst training, which includes 8 courses including public opinion analysis and judgment methods, public opinion crisis management and response. Those who pass the exam will be provided with the identification certificate of the public opinion analyst and the working certificate. Collect the opinions and attitudes of netizens, organize them into reports, and submit them to the decision makers. This is the "Internet public opinion analyst". At present, more than 2 million people are engaged in this occupation. According to reports, these people are distributed in party and government propaganda departments, portals, commercial companies and other institutions." (Gao, 2013)

The CCP governs a country of over 1.4 billion citizens and therefore, easily has the 'human power' to operate a massive internet police force as described above.

China views cyberspace as a national security matter and desires legitimacy for its "information control regime", the cyber sovereignty model (Alsabah, 2016). China's approach to cyber governance is consistent with its current political policies, both domestic and foreign. At home, China strives for societal cohesion and under Xi Jinping,

has increased its nationalist rhetoric. Outside its borders, China has become an increasingly involved actor in international organizations and has used its rise to influence everything from trade to technology. On the international stage, China has been the leading proponent of the state sovereignty model of cyber governance and is aiming to recruit other states to diverge from the multi-stakeholder approach, which China views as expansion of American hegemony into cyberspace.

Russia and the RuNet

Following China's example, neighbor and strategic partner, Russia has increasingly tightened its internet policies and has set a clear path towards the cyber sovereignty model. Compared to the United States and other western states, Russia was late to the internet. The internet in Russia is often referred to as the RuNet and started out slowly with only "a small number of Internet service providers... in the early 1990s" and the "RuNet was known to very few Russians" (Bowles, 2006, p. 21). Russian society was uncertain about the RuNet and its utility, it was seen as "a mere adapted outpost of American technology" and therefore did not gain traction until the mid-90s when Microsoft released Windows 95 which included "the Microsoft standard for Cyrillic encoding" (Bowles, p. 21). As Russian language websites began to be created, slowly more internet users got online. Over the next few years and into the new millennium, internet usage increased and by 2018, just over 80% of the Russian population was connected to the world wide web (see figure 6).

In Russian society, as in much of the world, the internet has become an integral part of society and government and Russia has looked to the types of controls that China has taken in governing their portion of the internet. Russia has also been pursuing a cyber sovereignty model, similar in nature to that of China. By pursuing the cyber sovereignty model, Russia wants to (1) “create a mechanism for effective surveillance of the internet within its borders; (2) “become key regulator of the internet in Russia”; and (3) expand the state-centered model of the internet at the international level” (Epifanova, 2020). On May 1st of 2019, President Vladimir Putin signed Russia’s ‘sovereign internet’ bill into law and according to the Russian government, the new law is “supposed to help the government provide a secure and uninterrupted internet connection and to protect Russian people’s interests” (Rossokhovatsky & Khvostunova, 2019).

Figure 6: Russian internet users as % of population, 1995-2018

Source: The World Bank 2018

Russia's portion of the internet is just like any other networked section of the internet, it is a network within a network that resides within Russian borders. This 'sovereign internet' law ensures that Russian ISPs, messengers, and email providers all work with the government to close off the RuNet from the rest of the internet at the government's request. This is achieved by Russian ISPs installing hardware at internet nodes at points of entry into Russia territory that would cut off internet traffic from external networks, creating an insulated and 'sovereign RuNet'. Beyond the control of traffic at internet "choke points", Russia is further distancing itself from ICANN by overseeing domain name registry functions for Russian sites (internet domain addresses which end in .ru and .рф) and this "forces all domains in the .ru zone to be hosted in Russia" (Nikkarila & Ristolainen, 2017, p. 2) and gives the government complete control over content and traffic within its borders.

Both Russia and China have chosen to reject the multi-stakeholder approach and forge their own path within their borders, but they also want to serve as pioneers in this model of cyber governance and recruit other states to reject the West's model. This push towards cyber sovereignty is more than just political ideology, there are also the politico-economic factors at play. The Chinese-Russian cyber alliance recognizes that their multinational companies are losing market share to American and European companies, and they want what they view as their rightful place on the international stage. From the Russian and Chinese perspectives, there is a "global monopoly of a few large companies and the United States in software and related fields" (Russia's Presidency in BRICS,

2015). At the October 2015 meeting of BRICS, Russian telecom minister, Nikolay Nikiforov said:

One of the key issues on the agenda concerns what joint efforts should be taken, without introducing any sanctions, so that national IT companies of the BRICS countries could take their rightful place on the market of the BRICS countries and, ideally, on the global market. (Russia's Presidency in BRICS)

For Russia and China, the cyber sovereignty model works well, not only for security reasons but also for political and economic factors. China's SOEs and Russia's oligopoly are perfectly suited actors for this model of internet governance. Close coordination between government and enterprise, without interference from civil society, allows for this model to operate without debate or checks and balances.

The State Sovereignty Model: What works and what does not

The cyber sovereignty model clearly appeals to non-western autocratic states, China and Russia being two of the best examples. President Xi has recently consolidated power within the CCP and has removed term limits, a move that President Putin is in the process of achieving. It seems only natural that a consolidation of power over the internet within their respective countries would be expected. To many in the West, this type of control over internet content and accessibility would be unimaginable, there are some benefits, primarily strategic for this model.

By controlling content, filtering out voices of dissent, states who subscribe to this model can mitigate (or eliminate) the digital reach from any challengers to power (as was

done to the China Democratic Party). In addition to suppressing domestic social dissent, the state can thwart misinformation campaigns and external information flows, which could influence domestic thought. The cyber sovereignty model also allows enhanced security measures to protect the state's critical infrastructure. The move to disconnect the RuNet from the rest of the internet is a defensive measure that in the event of a major cyber-attack, Russia could sever internet traffic to stop or slow down the use of cyberweapons on domestic networks.

Apart from these two main benefits, the downside is much more impactful. The focus on maintaining power and security comes at a cost, especially in a globalized world system. With China and Russia so closely aligned on internet government policy, they are isolating themselves from the other cyber powers who adhere to the more open, multi-stakeholder model. Despite the obvious downsides, China and Russia continue to advance the cyber sovereignty model to the rest of the world and present it as a path to self-determination, free of the influence of American hegemony in cyberspace. Rather than rely on American cyber technology, the Russia-China cyber-alliance has forced them to rely on themselves and each other as they chart their own path. Success on this front has been limited, and while China and Russia have succeeded in establishing their model domestically, the only publicly acknowledged subscribers they have acquired are Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, who partnered together put forth "the international Code of Conduct for Information Security to the United Nations" in 2015 (CCDCOE, 2015).

The state sovereignty approach to cyber governance is rooted in political ideology, led by, perceived “strongman” states and is synonymous with overreaching government intrusion into privacy. The cyber sovereignty model, whether it be China’s Golden Shield tactics or Russia’s Sovereign RuNet approach, is built on a foundation of security and control. The next section will discuss the importance of cyberwarfare as it relates to internet governance.

Cyberwarfare and Cyber governance

The discussions regarding the multi-stakeholder approach to internet governance tend to center around technical and economic issues, while the state sovereignty approach does the same but also emphasizes the importance of security issues. That is not to say that the multi-stakeholder approach does not consider security while promoting an open and free internet, they certainly do (Team Telecom’s oversight role is just one example), but within the state sovereignty model, security is a core aspect and benefits from a centralized power structure. This section will address the importance of cyberwarfare in the international system using, what I consider to be two of the most significant cyber-events to date; (1) the cyber-attacks on Estonia in 2007, and (2) the NSA cyber surveillance program which was publicly revealed in 2013.

Political tension meets cyberwarfare in Tallinn

The first known cyberattacks involving the state as a target occurred in 2007 in Estonia. What began as a societal issue between ethnic Estonians and ethnic Russians in

country, rapidly escalated into a cyber-attack on the state and its citizens. In 2007, Estonia was one of the most cyber-integrated societies in the world, with most everything shifting to online platforms, such as “government communications with its citizens, voting in elections, filing of social security applications, banking” and its citizens were issued electronic ID cards allowing them online access to these services. Estonia was an early adopter of ICTs and served as an example of what ICTs could achieve for an information society that embraced the ideals of a free and open internet. Conversely, Estonia’s dependency on ICTs also made it vulnerable to malicious actors.

In the aftermath of WWII, the USSR erected a statue in the center of Estonia’s capital Tallinn. The bronze statue depicted a Russian soldier and was titled “Monument to the Liberators of Tallinn” and for Russians, it was a symbol of victory and pride; for ethnic Estonians, the statue was a reminder that they were not free, but instead an occupied country. Finally, in 2007, the government of Estonia wanted to move the statue to the edges of the capital city and many Russians in the country and outside were outraged. The tension was “exacerbated by false Russian news reports claiming that the statue, and nearby soviet war graves, were being destroyed” (McGuinness, 2017). On April 26th, protestors took to the streets, and on April 27th the country’s online infrastructure began to be attacked. The attackers utilized a technique called distributed denial of service (DDoS) attacks, in which they employed botnets. The botnets (a combination of terms: robot and network) are a collection of “hundreds of thousands of individual computers from around the world that had been hijacked previously by

hackers” and these computers “known as zombies, could be made to repeatedly flood designated Internet addresses” thereby overwhelming the sites’ servers and shutting them down (Davis, 2007). The attacks crippled the Estonian government and society because of “the degree to which it had integrated internet-based solutions into most aspects of public daily life” (Haataja, 2017, p. 160); “Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic” (McGuinness, 2017).

In addition to the botnet attacks, ‘script kiddies’ were mobilized to perform large scale, coordinated “ping attacks”. This is a technique, similar to the botnet attack, but rather than deploying hundreds or thousands of enslaved computers, ‘script kiddies’ (individual low skilled hackers), would ‘ping’ website servers. One ping will do nothing to a server, but when “repeated hundreds of times per second...the pings could overwhelm a server” (Davis, 2007). The script kiddies were mobilized via online Russian speaking chat rooms and organized to “attack at the stroke of midnight on May 9th” (Davis). Between the script kiddie attacks and the botnet attacks, Estonia’s digital infrastructure ground to a halt and the attacks continued for weeks.

So, who was to be held responsible for the attack on Estonia? Would other NATO members fulfil their duties under its collective defense principle, Article 5 of the founding treaty? Evidently, these questions raise more problems than solutions. How to go about attributing the attacks to a particular state? There was ample evidence that the attacks on Estonia were politically motivated and the most obvious culprit was Russia.

Upon cyber forensic investigations, it was determined that the botnet attacks originated “from Russian IP addresses, online instructions [to low level hackers] were in the Russian language and Estonian appeals to Moscow for help were ignored” (McGuinness). Regarding NATO’s response, they did not respond with any collective defensive measures. It was determined that a response was not required because the criteria for an attack was not met; triggering Article 5 would require a “major loss of life equivalent to traditional military action” (McGuinness). Despite the evidence, Russia denied any involvement and without any pressure from NATO, the culprits escaped justice.

The events described above were some of the most important for the development of cyber governance debates in the international community. It was in part because of these attacks in Estonia that the NATO Cooperative Cyber Defence Centre of Excellence was established in 2008 and the Tallinn Manual was created. The Tallinn attacks made states aware that while cyber technologies have the potential to advance their societies and economies, there were also potential areas that could be exploited by malicious actors.

The events in Estonia also highlight three key problems when dealing with states and cyber security issues: (1) the challenges of attribution in cyberspace; (2) is it considered an attack if kinetic damage was not inflicted?; and (3) what is a measured and appropriate response to cyber-attacks? The authors of the previously discussed Tallinn manual 2.0, have attempted to provide clarity to these issues but as discussed earlier, global agreement has not been achieved.

The NSA and the Snowden Leaks

In the summer of 2013, it was revealed that the United States' National Security Agency was actively surveilling internet and telecommunications traffic. The fact that the NSA was spying is not a surprise, that is part of their agency mission; what makes this case significant was the scale of the NSA collection and that the targets of collection were foreign allied states, as well as enemies. The revelations came to light in June of 2013, when then a CIA systems analyst contractor, Edward Snowden leaked thousands of documents related to cyber operations conducted by the NSA, which showed an extensive network of tools and methods through which the NSA was able to collect internet and telecommunications data from across the world.

The 'Snowden leaks', as they have become known, detail several methods of data collection. For the purposes of this research, I will focus on two critical revelations: (1) the NSA's PRISM program, and (2) the 'tapping' of fiber-optic internet cables. Both cases will demonstrate western hegemony in cyberspace, a concern of both Russia and China and explain their reasoning for their international push towards the cyber-sovereignty model.

The PRISM Program

The NSA's "Planning Tool for Resource Integration, Synchronization, and Management" (PRISM) program is a "data tool designed to collect and process foreign intelligence that passes through American servers" (Drefuss & Dreyfuss, 2013). Among

the leaked documents, published by the *Guardian*, are internal NSA presentation slides (see figure 7) which explain that while the world's internet is a network of networks, “much of the world's communications flow through the U.S.” (NSA Special Source Operations, 2013).

Figure 7: NSA Introduction slide to the Prism program

Source: NSA Special Source Operations and published by The Guardian 2013

As previously mentioned, the internet, especially under the multi-stakeholder model, is comprised of public and private actors, and through a partnership with the private entities, the PRISM program was able to acquire data from ISPs (e.g. Verizon,

AT&T) and content providers (e.g. Google, Facebook, Microsoft). The data collection worked in two ways: (1) legally requiring companies to turn over data at the government's request, and (2) requiring ISPs to intercept specific data travelling via their networks, a process known as "upstream" collection (Franceschi-Bicchierai, 2014). The companies who join the PRISM program are not forced but asked to participate and are protected legally because they fall under American jurisdiction. The companies who took part (as of October 2012) and their "collections details" are presented in figure 8. The PRISM program was not a subversive and illegal operation, in fact it was subject to FISA warrants and oversight but because of its sensitive nature, the operation was kept "top secret". Through PRISM, the government was able to surveille everything a target was doing and with whom they were communicating. The purpose was to protect the US from another 9/11-type scenario, but targeted data collection turned into mass surveillance, which included citizens and leaders of many countries, including some from allied states.

PRISM did not just operate with the cooperation of American companies, but allied states also unknowingly participated. The NSA, having existing relationships with allied intelligence agencies, went to great lengths to acquire any and all information they wanted. The NSA would reach out to allied states (e.g. Germany, Sweden, France, Netherlands) and request "collaboration in relation to reasonably legitimate matters (mainly concerned to antiterrorism and organized crime)" and once they had access to their systems would deceptively "introduce tools into their collaborators' systems" (Bauman, et al., 2014).

Figure 8: Private sector actors and the data they collected via PRISM

Source: NSA Special Source Operations and published by The Guardian 2013

US-UK Partnership: Tempora

The second revelation from the Snowden leak that is particularly significant to this research is the unveiling of British involvement in mass surveillance. In an operation code named “Tempora”, the Government Communications Headquarters (GCHQ), NSA’s British counterpart, was found out to be placing “data interceptors on fibre-optic [sic] cables that carry internet data in and out of the UK” which allowed them “to directly

access large amounts of global internet data” (Shubber, 2013). At the time of the leaks, GCHQ data interceptors were present on approximately 200 fiber-optic internet cables (that is about half of the cables in existence today, and it is not clear if more have been installed since the leaks). The interceptors were installed with the cooperation of the cable operators and were described in the leaked documents as “intercept partners” (MacAskill, Borger, Hopkins, Davies, & Ball, 2013). These intercept partners include some of the largest ISPs not only in the UK but the world: Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute (Franceschi-Bicchierai, The 10 Biggest Revelations From Edward Snowden's Leaks, 2014).

Tempora allowed the GCHQ and partners at NSA to “look for information on targets” and the information was shared between agencies. The NSA and GCHQ cooperated together in a mutually beneficial arrangement, by sharing information, they were able “to bypass domestic restrictions on intelligence gathering... the NSA isn’t bound by UK restrictions on surveillance of UK citizens and GCHQ isn’t bound by US restrictions on surveillance of US citizens” (Shubber). Although GCHQ’s Tempora received less attention in the media, compared to the NSA’s PRISM program, they are both crucial to understanding the opposition to the American-led multi-stakeholder model of cyber governance.

The Consequences of Prism and Tempora

While PRISM and Tempora gave the United States a cyber advantage in gathering intelligence on their targets, the public confirmation of their existence damaged US credibility and gives credence to the Russian “narrative that American democracy is as politically corrupt as any other form of government” (Roth & Priest, 2016). Russia and China are further supported in their claims of American hegemony in cyber-space, making their argument for the state-centric model of cyber governance more legitimate. Also adding to criticisms of the multi-stakeholder model, it cannot be argued as well that a system of checks and balances works in this system because actors within the model cannot deny the governments under which they operate and fall under their jurisdiction.

In addition to the above consequences, the multi-stakeholder model, which purports to promote a free and open internet appears to be somewhat similar to China’s surveillance within their great firewall. The difference being less censorship and an alternative framing of their narrative.

Is IR theory applicable to cyber-relations?

Throughout the modernity of international relations, the two most ubiquitous theories used to explain and predict world events are realism and liberalism. The two paradigms are unique and yet related in many ways. The following section will provide a brief overview of each world view and then examine their relevance to international relations in the digital age.

Realism, inspired by the Hobbesian tradition, views the world as operating in a state of anarchy where states exist only for self-serving purposes. In this system of anarchy, realists only recognize states as primary, states are treated as single unitary actors, and are principally concerned only with great power states. As such, and by applying the second image analysis, any state is treated as a black box with internal decision making disregarded (Waltz, 1959). There is no recognition of other levels of analysis within the realist framework, other than states and this makes for a simple “top-down” method of governance in foreign affairs. Individuals are not considered (first image according to Waltz) nor are civil society or international governmental organizations. As a result of states being self-interested and in a state of anarchy, realism is power-centric with a particular emphasis on military power (hard power) and “survival is the number one goal” (Mearsheimer, 2014). While realist scholars do not dismiss latent power, they recognize it only as a means of increasing hard power. This makes powerful states cognizant and cautious of less powerful states who have “large populations and rapidly expanding economies, even if these states have not yet translated their wealth into military might” (Mearsheimer).

Being so concerned with power, realism seeks to find peace through might. Supporters of the realist tradition are often misunderstood as war-mongers and while it is true that there is a heavy emphasis on hard power, the theory focuses on attaining balance and peace by deterrence, and/or reducing challenger states’ capabilities to wage war, thus achieving peace (or so the idea goes). Through the realist lens, multi-polarity in the

international system is a recipe for conflict, while a bi-polar scenario offers more stability there is still conflict and smaller peripheral states are forced to fall in line with one camp or another. The ideal scenario for realism is a unipolar scenario with the hegemon sitting at the top, establishing peace, order and economic prosperity (Webb & Krasner, 1989). This approach is most well known as hegemonic stability theory (HST).

Regarding hegemony, realism's emphasis is again related to a state's hard power capabilities and how a particular state can project that power. The idea being that a hegemonic state must be able to coerce other states into order through military might or the threat of such might. According to offensive realists, such as Mearsheimer, physical proximity to rival states matters because of the extent of the hegemon's physical reach. He claims that a true global hegemon could not become a reality because the distances would be too great for a single country to achieve hegemony globally. The best case scenario is a regional hegemon who is "so dominant in their neighborhood" that "they are free to roam around the globe and interfere in other regions of the world" (Mearsheimer).

Liberalism shares some basic assumptions about the world with realism but differs in key areas. Liberalism is also built on a "top-down" approach but recognizes not only states but international governmental organizations (IGOs) as well. While realism is founded on the work of Thomas Hobbes, liberalism derives its founding principles from Immanuel Kant. Kantian principles include liberty, democracy, human rights, and institution building. In liberalism, the world is viewed through a more optimistic lens where cooperation is favored over the coercive methods employed by realism, and

through cooperation, peace and prosperity can be achieved. This is achieved mostly via economic incentives. These incentives discourage traditional conflict by making warfare an expensive endeavor, primarily by weakening trade and thus inflicting major economic loss on the participants.

While liberalism does not discount the importance of hard power, soft power is favored and preferred as a means to foreign relations. Soft power, “is the ability to obtain preferred outcomes through attraction rather than coercion or payments” (Nye J. S., 2009). When dealing with the notion of hegemony via the liberal lens, the concept is not applied to a single state but rather international regimes through which states participate and conform (Koremenos, Lipson, & Snidal, 2004). Adhering to liberal principles and participating in IGOs, like-minded states cooperate, economic and social interdependence is established, and peace is obtained; and these interdependent states form a liberal zone of peace (Buchan, 2002). This aspect of liberalism is best described by institutionalist regime theory (Hynek, 2017).

Applying Realism and Liberalism to cyberspace

In their respective ‘primes’ both realism and liberalism have served as prescriptive and predictive tools to explain past and future international affairs. They are shaped by the world in which they were created (i.e. post-WWII cold war eras.) However, the complexities of the introduction of cyber technologies have altered the

international stage to such a degree that realism and liberalism cannot, in their current form, prescribe or predict accurately.

For instance, the claim found in realism that distance is a key factor for hegemony is undercut by cyber technologies. Oceans separate the United States from much of the world, and so to a realist, this means that the US has a strategic advantage where rival states could not effectively attack them. Cyber capabilities change this assumption by eliminating distance as a factor. With the world connected by fiber-optic cables, rival states or even lone-wolf hackers could attack from across the globe without having to mobilize many resources in the traditional sense. Realism does not account for this. In fact, realism dismisses cyber technology as a legitimate threat. If an attack does not involve kinetic destruction or severe loss of life, the attack never happened. Additionally, realism, a theory built on the notion that “the life of man” is “solitary, poore [sic], nasty, brutish, and short” (Hobbes, 1929, p. 97). does not consider the individual for analysis, but rather applies its concept of man to the state and further dismisses non-state actors.

Liberalism also falls short in explaining foreign affairs in the digital age. One of the key points to liberal theory is that interdependent states make allies and form a zone of peace. This argument is undercut by the revelations that the NSA and GCHQ were actively intercepting internet traffic from their allies not just specific enemy targets. While it is true that the US and UK are liberal democracies and allies, their collaboration in this matter is a dyadic one where the rest of the allied states were not involved, and

some were even duped into participating without understanding the subversive tactics employed by the NSA and GCHQ.

I contend that there are ontological lessons to be drawn from both realism and liberalism, but neither seems to fully appreciate the seismic change that ICT has played on international relations. On the surface, realism seems to lend itself to the cyber sovereignty model, while liberalism is more closely reflective of the multi-stakeholder approach; but there are several layers in-between that require further explanation. The following section will present an adaptation of realism and liberalism, updated for the digital age.

Governance and Security in Cyberspace (GSC) Theoretical Framework

The previous chapters have explained the multi-stakeholder and cyber sovereignty models of internet governance, as well as the significance of including cybersecurity when discussing either model of governance. Here I will present specifically how cyber governance and security have altered international relations theories and how they must be updated. I propose the following framework, which I have termed the theory of Governance and Security in Cyberspace (GSC). What follows is my own original theory for understanding international relations in the digital age (see table 4). The GSC framework is informed by Daniel Nexon and Thomas Write's analysis of international system dynamics, the reconceptualization of power by Michael Barnett and Raymond Duvall and the system theorization of Quddus Z. Snyder.

Table 4: Realism, liberalism assumptions versus GSC theoretical framework

Views	Realism	Liberalism	GSC
Human Nature	Pessimistic: Hobbesian principles	Optimistic: Kantian principles	Neutral: Irrelevant
Key actors	States (top-down)	States, IGOs (top-down)	States, MNCs, IGOs, Technical bodies (ICANN), Private firms and Individuals (multi-tiered)
International system	Anarchical	Anarchical, but growing world order	Hierarchical, but allows for challengers
Main cause of conflict	States are self-interested	No central authority to regulate competition	Economic self interest
Power considerations	Projecting and using hard power	Encouraging interdependence and cooperation, prefer soft power	Power is decentralized Attracting others to governance model but backed by hard power. (smart power)
Best path to peace	Hegemon establishes order (zero-sum)	Interdependence maintains peace (zero-sum)	Deterrence with tolerable micro-aggression (positive-sum)

Assumptions, and actors in cyberspace

After analyzing the multi-stakeholder approach, the cyber sovereignty model and events related to cyber security, I have determined that realism and liberalism are not fully equipped to understand IR as it relates to cyber relations. Let me begin with the perception of human nature; realism offers a pessimistic view while liberalism offers an optimistic view. My proposed theory for understanding IR in the digital age views human nature as irrelevant. It is perfectly conceivable that a liberal democracy will at some point in the near future, abandon the multi-stakeholder approach for a hybrid approach where it

decides to ‘secure’ its digital borders, much like what Russia is in the process of doing today, but retains its Kantian values through participations in IGOs and its economic policies. The age-old debate about human nature and its implications on the international system are not easily applied to cyberspace and thus my theory concludes that it is ultimately a non-factor.

The old paradigms in IR consist of top-down approaches to understanding world politics, however, examination of internet models of government and cybersecurity have illustrated the fact that there are several key actors in this arena and not all are situated at the “top”. My theory presents a multi-tiered composition of actors, consisting of states, MNCs, IGOs, technical bodies, and individuals. Actors in this theory consist of different levels of influence and capabilities; there are several potential actors but there are differing levels of significance (a hierarchy of cyber capabilities).

Beginning with the most formidable actors in cyberspace, I will now explain the role and hierarchy of states. Tier 1 states are highly technically capable and have abundant resources to operate offensively as well as defensively in cyberspace. States who fall under the Tier 1 category can claim “technology champions”, and telecom giants based within their borders. The first and most obvious example, is the United States; a Tier 1 state who is home to tech champions such as Microsoft, Google, Facebook, Verizon, AT&T, just to name a few, has significant capabilities and reach. Leveraging these tech champions in addition to an already enormous government cyber apparatus, places the United States firmly in the Tier 1 category. Another example of a Tier 1 state

is China, who also possesses significant cyber capabilities and is home to its own tech champions such as Huawei, Baidu, Alibaba, China Mobile, and Xiaomi. Tier 1 states such as the US and China can project their power and influence and are the strongest proponents of their preferred system of cyber governance.

Tier 2 states are also highly capable in cyberspace and are actively developing their cyber capabilities but have not reached the level of sophistication that Tier 1 states have achieved. States who fall into this category do not possess any homegrown tech champions and the development of cyber capabilities is done through government agencies or military and relies on assistance from external tech champions. A prime example of a Tier 2 state is Iran, who began to develop their cyber capabilities as methods of “domestic surveillance and control” in response to the “Green Revolution” of 2009 and developed offensive capabilities in response to the ‘Stuxnet’ attack on its nuclear enrichment facility at Natanz (Lewis, 2019). Iranian cyber-warriors are highly skilled members of the Islamic Revolutionary Guard Corps (IRCG) and the Iranian Cyber Army (ICA) who, at present are capable of highly technical attacks but do not yet have the resources to develop new and unique cyberweapons (Anderson & Sadjadpour, 2018). Tier two states, lacking their own tech champions will partner with external actors, the way Iran and Huawei are reported to have done. Huawei is accused of providing telecom equipment to Iran through a series of shell companies to avoid violating sanctions. Furthermore, Iran (a Tier 2 state) in at least one series of events, has chosen to bandwagon with China (a Tier 1 state), with coordinated attacks against a common rival,

the United States (Perlroth, 2019). Tier 2 states will most likely bandwagon with Tier 1, like-minded states, rather than invest massively to develop domestic tech champions and telecom giants.

Finally, concerning states, the Tier 3 actors possess little to no cyber capabilities and they should not be ignored, but rather recruited to a preferred model of internet governance. Given the impact that ICTs have played in connecting the world, this technology is here to stay, and Tier 3 states will eventually have to decide what camp they will fall in with. Tier 1 states will offer their models as the best option for Tier 3 states reminiscent of the East vs West, capitalism vs communism Cold War era. Factors that will decide which model of cyber governance a Tier 3 state chooses will depend on two main indicators: (1) system of domestic government and (2) economic cyber development (this will be addressed further in the following sections). Liberal democracies are more likely to fall in line with the western led multi-stakeholder model, while autocratic states will favor the cyber sovereignty model. Most likely, Tier 3 states will aspire to advance to Tier 2 status and given that the economic barriers are low for entry into cyberspace, Tier 3 states could advance their cyber capabilities in a relatively short period, unlike building up a traditional military force.

Adjacent to states are the combination of MNCs, IGOs, and technical bodies (e.g. ICAAN). These three groups form the second column of actors found within the GSC's theoretical framework. The role of telecom giants and internet content providers is critical to the entire internet. Without them, the rapid expansion of ICTs would not have

been possible. They are not only responsible for creating physical cyber infrastructure but also maintaining the lines through which internet traffic flows. They take on a role which, in terms of power dynamics, is lower than a Tier 1 state but ranked higher than Tier 2 and 3 states. Given the fact that the technologies that tech and telecom giants possess are simply too technically advanced and resource abundant, a Tier 2 or 3 state is not able to equate.

To further make this point, let us return to the Tier 2 state example of Iran. According to the latest data available from the World Bank, Iran's Gross Domestic Product was approximately \$454 billion in 2017 and is believed to have decreased since (primarily because of economic sanctions). If we compare Iran's GDP to the market value of the world's four largest tech companies, we see a staggering difference in wealth. As of January 2020, Google, Microsoft, Amazon, and Apple have all surpassed or are close to a trillion dollars in market value (Wakabayashi, 2020). All the wealth that these companies have produced is miles ahead of Iran and they do not have to support a population or secure any borders. These tech champions are not only wealthy but also enjoy the security provided to them by being US based companies. On the world stage, this gives them enormous influence but also makes them beholden to the US government (e.g. participation in the PRISM program) while still having enough independence to pursue investment overseas, thus placing them below Tier 1 states but above of Tiers 2 and 3 in terms of power and capability.

Intergovernmental Organizations, such as NATO and technical bodies, such as ICANN provide structure and commonality across borders in terms of cyber jurisprudence and technical architecture. Their existence creates stability but also creates points of contention. Any state who is not a member of a given IGO falls outside of the decision-making process; and while the work done by the UN GGE to create the Tallinn Manual 2.0 provides an interpretation of international law, it has no authority or capability to act or enforce its rulings. ICANN also provides a common good but being that this body is based in the United States, rival states will resist ICANN control of the Domain Name System. Essentially the existence of these actors forces any state who does not wish to subscribe to the multi-stakeholder model to create an alternative version (like Russia has done by exerting control over Russian domain names ending in .ru).

The third column of actors described in the GSC framework is comprised of small private cyber security firms and individuals. Actors in this grouping have a small physical footprint but are potentially capable of rivaling capabilities of states with regards to cyber-weapons and cyber-attacks. Small private firms such as NSO Group, Verint, Elbit System, and Hacking Team develop malware, spyware and other types of cyberweapons to sell to private and sovereign clients (Franceschi-Bicchierai & Cox, 2018). These companies are at the forefront of the marketization of cyberwarfare. These private firms are significant because they can provide Tier 1 and 2 states with cyber-products ready to purchase rather than having to invest their own resources to develop the needed tools. The Israel based NSO group's PEGASUS malware allows the attacker "full access to a

target's phone, including their camera and microphone" and "according to Citizen Lab at the University of Toronto, NSO's Pegasus software has been detected in 45 countries" (Field, Chowdhury, & Sanchez, 2019). Tier 3 states could also become clients of these private firms as a means for rapid deployment of cyberweapons which they do not yet have the ability to develop.

One of NSO's rivals, Hacking Team, an Italian based firm, developed a remote-control service (RCS) named "Galileo". Once deployed, the Galileo program was able to "siphon off data and listen in on communications before they have been encrypted" essentially capturing all computer activity of the target without the target's knowledge. One of Hacking Team's most notable clients was the Federal Bureau of Investigation, who bought Galileo as early as 2011 (Cox, 2015). The FBI's use of such malware highlights the dangers that the proliferation of cyberweapons presents. Developing these weapons is not as resource intensive as the traditional tools of warfare or espionage but can cause serious damage if used by malicious actors.

Aside from the private firms, individual hackers are included in this category because of their small physical footprint and potential capability for damage. Recall the cyber-attacks on Estonia in 2007. The attacks which shutdown the state's ability to function was not the result of a deployment of a highly sophisticated cyberweapon but rather a collective effort of motivated individual hackers. It is for this reason that the GSC framework considers the role of the individual as an actor. The tools employed by these

hackers may not always be the most technically sophisticated but can have devastating consequences if attacks are coordinated.

The Cyber International System

The international system is viewed as anarchical by realism and liberalism, here again the GSC framework differs. Upon analysis of the various models of cyber-governance the international system in cyberspace is a system of competing confederacies with hierarchical actors found within. While at first glance, it seems that the internet is a wild west landscape where anything goes, it is apparent that previous power structures have translated to cyberspace. There are clear cyber-powers who can claim dominance over others, but power can shift in cyberspace, given the diversity of possible actors. Furthermore, the relative low cost to entry makes the rise of challengers more possible than through traditional political or economic structures.

While GSC proposes a hierarchal order to cyberspace, it is theorized here that the system is not strictly a “top-down”, structure but rather one where the system is dependent upon actors across the various Tiers and columns to cooperate. These actors, however, do not operate independently and are subscribers to a particular model of internet governance. Adapting Quddus Z. Snyder’s “grand-theory of system structure”, GSC proposes that the international system as it relates to cyberspace is a system of competing confederacies, represented by the multi-stakeholder and the cyber sovereignty models. Each confederacy contains the actors discussed above in a hierarchical structure

(see figure 9). Snyder explains that in a confederacy, “the leading powers are united both by a structure of mutual dependence and affinity based on similarity and solidarity founded on a shared normative framework” (Snyder, 2013, p. 554). This dependency and affinity can clearly be observed with the competing models of internet governance. While Snyder focuses on states in the international system, the GSC framework considers the various other actors involved and their place within the hierarchy. This structure is similar to a constitutional order which centers around institutions but is organized and led by a hegemon through informal ties (Nexon & Wright, 2007) (see figure 10).

Figure 9: International System proposed under GSC theoretical framework

Source: Savvides 2020

Figure 10: Constitutional Order led by Predominant Power linked to others via informal ties

Source: Nexon and Write 2007

The GSC framework proposes that cyberspace has a hierarchical power structure with Tier 1 states at the top of the order. As discussed previously, states in this category possess dominant cyber capabilities and that translates into the ability to influence other states to their preferred models of cyber governance. Tier 2 states will bandwagon with a given cyber-power (Tier 1) depending on preexisting political and economic factors. However, the international power structure of cyberspace is not static and allows for challengers (other states) and threat actors (private firms and individuals), from a rival confederacy to be relevant.

At the surface level, conflict within this system is, driven by states, but more than just political rivalries, Tier 1 states are bolstering the reach of their respective tech champions by pursuing more actors to join their model of internet governance. Each

confederacy sees the potential for political and economic dominance if their preferred system of governance wins out. In the same way that political economy fueled the Cold War (at least in part), today's cyberspace rivalries are also economically driven. As the dominant multi-stakeholder model continues to grow, proponents of the cyber sovereignty model are increasingly squeezed out of the global market share. Cyber-conflict can occur when the Tier 1 states, feel threatened that their respective tech champions will be contained to smaller markets and/or restricted from growth.

We can see this form of conflict in the events surrounding the global development and implementation of 5g technology. The race for 5th generation telecommunications dominance is one layer of the conflict between confederacies. As an example, let us briefly examine the case of US based champion, Verizon versus the China based champion, Huawei. Each champion is vying for global market share to build their brand of 5g networks. At the individual level of analysis, 5g communication is a marketable product, offering faster internet speeds for consumers using mobile devices and home and business internet services. The market for internet service is in high demand and there are significant profits to be made; in the US alone, the top five telecom companies had a combined revenue of \$383.69 bn in 2018 (Statista, 2019). The stakes are high for these champions to corner the potential revenues associated with 5g but are even higher, given the applications for the industrial sector; 5g technology makes it "possible to manage factories remotely in real time" and "is also a key ingredient in making driverless cars a reality" (Cooper, 2018).

Beyond the consumer and industrial levels, there are also national security implications for 5g, and states want to ensure their champions have the advantage. Tier 1 states, regardless of their chosen cyber governance model, will use whatever means necessary to promote and support their tech/telecom champions. The United States has gone to great lengths to protect and bolster their respective champions in the race for 5g. On May 5th of 2019, the Bureau of Industry and Security (BIS), an office within the US Department of Commerce, added Huawei “and its affiliates to the Bureau’s Entity List” (Bureau of Industry and Security, 2019). Being added to the Entity List means that “The sale or transfer of American technology to a company or person on the Entity List requires a license issued by BIS, and a license may be denied if the sale or transfer would harm U.S. national security or foreign policy interests”, essentially restricting Americans from doing business with Huawei (Bureau of Industry and Security, 2019). Huawei is the world’s “largest 5g equipment manufacturer” and the United States is skeptical of their intentions given the fact that “a Chinese intelligence law that requires companies and citizens to participate in state intelligence work if requested, including sharing data with the government” (Miller, 2020).

Most recently and in addition to their inclusion on the Entity List, US lawmakers have introduced the Utilizing Strategic Allied (USA) Telecommunications Act which “would set aside \$750 million within a grant program... to help support the deployment and use of 5G networks in the U.S.” (Miller). This case highlights the dynamics at play when dealing with the source of conflict in the international system as it relates to

cyberspace. On the surface, there is the narrative that this is a national security issue, but the more salient reasoning may be economic. Tier 1 states cannot allow their champions to fall behind competing champions because a Tier 1 state's 'cyber-power' is causally related to the economic success of their respective champions. When speaking about the USA Telecommunications Act, current US Senator, and co-founder of Nextel, Mark Warner put it best by saying:

Every month that the U.S. does nothing, Huawei stands poised to become the cheapest, fastest, most ubiquitous global provider of 5G, while U.S. and Western companies and workers lose out on market share and jobs. Widespread adoption of 5G technology has the potential to unleash sweeping effects for the future of internet-connected devices, individual data security, and national security. It is imperative that Congress address the complex security and competitiveness challenges that Chinese-directed telecommunication companies pose. We need to move beyond observing the problem to providing alternatives for U.S. and foreign network operators (Warner, 2020).

The race for 5g dominance illustrates the fundamental cause of conflict in cyberspace which is economically driven. The economic self-interest of Tier 1 states is the main driver of conflict and through their tech/telecom champions, states advance their capabilities in order to strengthen their respective confederacies.

Power in cyberspace

The concept of 'power' in international relations theory is a somewhat controversial one, with varying interpretations of the concept. Several interpretations of power exist, some labeled as: hard, soft, smart and sharp power, and while they each offer their own unique explanation for the concept in the international system, none agree

completely no do they fully encapsulate the concept as it applies to cyberspace.

International relations has examined the concept of power from different perspectives but

“the realist approach remains the industry standard” (Barnett & Duvall, 2005, p. 8),

which is to say that there is an emphasis on material resources as a key metric of power.

International relations scholars tend to understand power through two basic conceptual

lenses: “social relations of interaction” and “social relations of constitution”. Barnett and

Duvall explain:

This conceptual distinction between power working through social relations of interaction or in social relations of constitution tracks fairly closely with a distinction that frequents the literature on power: “power over” and “power to.” Concepts of power rooted in action and interaction point to actors’ exercising control over others; they are, then, “power over” concepts. Concepts of power tied to social relations of constitution, in contrast, consider how social relations define who are the actors and what are the capacities and practices they are socially empowered to undertake; these concepts are, then, focused on the social production of actors’ “power to (p. 10).

How does the concept of power translate to cyberspace and the international system? Under the GSC framework, power is decentralized, and while Tier 1 states possess the most power, they are still forced to enter into power-sharing relationships with actors from their own confederacies. Building off the work by Barnett and Duvall, power in cyberspace is both “interactive” and “constitutive”. Between actors in the GSC framework, the dynamics of “power over” and “power to” can be found and applied to each column of the system.

The GSC theoretical framework offers the following definition of (cyber)-power to better understand the way actors and processes interact through the hierarchical structure defined in the above sections. Recall from the definitions section that cyberspace is not a virtual realm, nor is it a physical realm, but rather a combination of the two. What is considered virtual cyberspace cannot exist without physical infrastructure or actors to build the networks, maintain them, and interact with other actors. This combination of virtual and physical also translates to the concept of cyber-power. Also recall that under the GSC framework, the international system allows for challengers and therefore the power structure in cyberspace is more fluid than that of traditional IR theories. Under the GSC framework, cyber-power is the ability of an actor (in the physical realm) to use ICTs (virtual realm) across cyberspace to achieve desired outcomes.

GSC proposes that cyber-power is expressed through a combination of economic status and cyber-capabilities, but that power is somewhat fluid and less reliant on traditional metrics of 'power'. The wealthiest and most technologically advanced states (Tier 1 states) have the resources to control the flow of internet traffic, initiate crippling cyberattacks and cross the line between virtual and physical if so desired. They possess what Barnett and Duvall referred to as "power over". Given that Tier 1 states are much more technologically advanced than Tier 2 or 3 states, there is a global inequality in power but that does not mean that these developing cyber states cannot challenge a more powerful state. Actors in this stratum possess the previously mentioned "power to".

Tier 1 states, as leaders of their respective confederacies, exercise the most amount of cyber-power but given the nature of ICTs, even a ‘weaker’ actor could undermine a Tier 1 state. Cyber technologies have altered the concept of power by making attacks, disruptions, or confusing a higher ranked actor much easier and harder to defend against.

Peace in cyberspace

One of the most important questions that international relations scholars want to answer is “how to achieve peace?”, while realism and liberalism offer zero-sum prescriptions, where winner takes all, the GSC framework views peace differently and offers a positive-sum prescription. There will inevitably be conflict in cyberspace and the zero-sum approach does not translate as clearly to cyber technologies and the international system. To understand the process of peace through the lens of the GSC framework, we need to understand first that peace in cyberspace is not equal to peace in the physical world and conflict is inevitable because it acts as a method of deterrence.

From 2009 to 2019, there have been an estimated 500 “documented geopolitical cyber-attacks around the world” and the trend has been increasing with “a 440% increase in global documented attacks” over that time period (Robinson, 2020). These attacks, targeted states and were conducted by states and non-state actors (individuals and small groups). China and Russia accounted for just over 55% of these attacks, each carrying out 79 and 75 attacks respectively (see figure 11). These are just the attacks that were

discovered or disclosed and can reasonably be attributed to China and Russia, and it is likely that there have been more global attacks from many actors which have not been discovered or disclosed and are possibly still on going.

Figure 11: Origins of cyberwarfare attacks (excludes attacks of unknown origin)

Source: Robinson 2020

With cyberattacks becoming more prevalent, why has there not been retribution attacks or why has it not escalated to traditional military attacks? There are two significant points at play here: (1) the playing field is leveled, no one actor at present has total domination over cyber capabilities and Tier 1 states are each capable of major

attacks acting as a deterrence; and (2) no kinetic destruction enables attackers to act with little fear of reprisal or public outcry. The first point is best illustrated with the United States openly attacking the Russian electric power grid. In response to Russian election interference in 2015-16 and 2018 (mid-term elections), the United States has shifted its strategy from cyber defensive to a cyber offensive one and has placed “potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before” (Sanger & Perlroth, 2019). This is a clear signal to Russia and other rivals that cyber-attacks may not be met with traditional force but that they will be responded to. This signal is a deterrence factor which is “intended partly as a warning, and partly to be poised to conduct cyberstrikes if a major conflict broke out between Washington and Moscow” (Sanger & Perlroth).

To the second point, the battlefield is digital and therefore destruction in the physical realm is rare. The only known instance of physical damage occurring as a result of a cyberattack is the Stuxnet attack, first identified in 2010. In that case, the attacker(s) installed malicious code into the computer system which controlled the centrifuges at the Natanz nuclear enrichment facility in Iran. The Stuxnet case is extremely unique and even with this case, there has not been a traditional military strike in response to a cyber-attack. Traditional methods of warfare are costly, but cyberwar is relatively inexpensive and there is an relatively little threat of loss of life, therefore attackers are becoming increasingly emboldened (even state actors). Since cyber-attacks do not inflict kinetic damage to their victims, they are often a nuisance, or they go unnoticed altogether by the

general population. States will respond in kind and ironically establish peace through conflict, with each side trading attacks.

Iran's response to the Stuxnet attack did not utilize traditional means of force, rather they further developed their cyberwarfare capabilities and responded with a series of cyber-attacks that became known as Operation Cleaver. Iran targeted "energy producers and utilities, commercial airlines and airports, military intelligence, aerospace, hospitals, and even universities" in sixteen countries (Cylance, 2014) as a means to signal to not just the attackers behind Stuxnet but also to the rest of the world that Iran has arrived has a cyber-power and to deter any would be attackers.

This may seem like a description of a zero-sum scenario, but the GSC framework incorporates the significance of economic factors as well as traditional metrics of power and force. When we overlay the factors described in the above chapters, we see that the confederacies (while competing with one another) are each growing economically, advancing cyber infrastructure and lifting their respective tech/telecom champions simultaneously, which is a positive-sum scenario. Peace in the physical realm is not without conflict in cyberspace.

Counter Argument

This research has argued that traditional international relations theories, in their current forms, are not equipped to accurately prescribe policy or predict behaviors; however, some scholars do not view ICTs / cyber technologies as a "gamechanger" nor

do they accept that these technologies have changed the threat landscape as I have described in the preceding chapters.

In his article, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth”, Erik Gartzke challenges the notion that cyberwarfare is a major component of foreign policy. Gartzke, rooted in realism, proposes that in an anarchical world, cyber war is not a major threat but more of an inconvenience and that “the internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest” while also arguing that “cyberwar is unlikely to prove as pivotal in world affairs, and for developed nations, in particular” (p. 42). Also grounded in realism, Thomas Rid contends that despite the warning bells, sounded by policy and military leaders, a cyberwar has not, and will not happen. Rid defines cyber war using Clausewitz’s three main elements: (1) violent character, (2) war is instrumental, and (3) war is political in nature. Rid goes on to say that there has not been one instance of a cyber-attack meeting all three criteria and therefore a cyber war is not possible (Cyber War Will Not Take Place, 2012). Although, as I have argued, the nature of foreign relations and warfare has changed due to ICTs, scholars like Gartzke and Rid refuse to view ICTs as a “gamechanger” and prefer the traditional view that conventional warfare methods are still the ultimate form of power, while completely disregarding the significance of cyber governance structures.

Gartzke and Rid view the internet (and associated technologies) as if it is an independent variable of traditional warfare means, rather than conceptualizing it as a

separate and integral aspect of the international system. They focus only on cyberwar and fail to see the significance of governance in cyberspace. When examined through geopolitical lenses, cyber governance and cybersecurity are not two separate topics but rather inextricably linked. By their logic, these scholars would have us believe that traditional means of war are separate from governance in the physical realm, but they are not separate, so why would cyber governance be ignored when dealing with cybersecurity issues? This is the core problem with attempting to apply traditional IRTs, such as realism, to cyberspace; they simply do not translate effectively.

Gartzke's take on cyberwar also illustrates a fundamental flaw in realist logic, when applied to IR and cyberspace. In his article, Gartzke states that:

Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary. In many, perhaps most, circumstances, this will occur only if cyberwar is accompanied by terrestrial military force or other actions designed to capitalize on any temporary incapacity achieved via the internet" (p. 43), and that "for cyber aggression to have lasting effects, a virtual attack must be combined with physical intervention (pp. 58-9).

Additionally, Rid argues:

that the world never experienced an act of cyber war, which would have to be violent, instrumental, and – most importantly – politically attributed. No attack on record meets all of these criteria (Cyber War Will Not Take Place, 2012, p. 29).

Examining Gartzke's argument, and if we temporarily remove cyber governance from the equation, his position still falls short and is heavily reliant on conventional methods of conflict. For a cyber-attack to be effective, according to Gartzke, "terrestrial

military force” must be utilized in conjunction with a cyber-attack(s). This paper has illustrated that cyber-attacks can be effective at harming a rival state without the use of terrestrial military force. The GCS framework recognizes that military force (hard power) is an effective tool as a means to backup cyber warfare (exemplified by the Tier 1 States category) but it is not a necessary component to have a formidable cyber army (e.g. Tier 2 States such as Iran) and conduct successful cyber-attacks (e.g. Operation Cleaver). Rid’s application of Clausewitz to cyber technologies is a flawed effort. What Clausewitz theorized about conflict in the 19th century has little relevance when applied to cyberspace in the 21st century and while Rid remains firm in his belief in the three criteria of conflict, they are not applicable today.

ICTs have altered the threat landscape as well as augmented traditional geopolitical structures (multi-stakeholder model with liberal democracies vs cyber sovereignty model with autocracies and states with consolidated power structures), and as such, the arguments that the above scholars propose, are not accurate for prescription of policy or prediction of behavior in cyber international relations.

Conclusion

The preceding chapters have provided an analysis of the intricacies between networked communication (ICTs), models of cyber governance, watershed cybersecurity events, and the actors involved at all levels of analysis. The purpose of this research was to evaluate the relevance of realism and liberalism in regard to cyber technologies in the

international system and further evaluate their predictive and prescriptive abilities. It is clear that, in their current form, the classical paradigms of IRT are not adequate for understanding international relations in the digital age and I have offered, the Governance and Security in Cyberspace (GSC) theoretical framework, as a foundation for future study. Under this proposed framework, the international system is understood as an informal hierarchy, with recognition to a multitude of actors at every level of analysis and re-imagines the concept of power as it relates to cyberspace.

The GCS framework, also envisioned the international system (as it relates to cyberspace) as conflict between competing confederacies, exemplified by the multi-stakeholder and cyber sovereignty models of governance. These confederacies are led by Tier 1 states, but are not considered true hegemons, since they rely on actors from different levels of analysis, the most prominent being their respective tech/telecom champions. This research has established that cyber technologies are indeed a gamechanger in international relations and has done so by employing a multi-disciplinary approach, synthesizing concepts and processes from international law, technical fields, and international relations. In doing so, has also served to bridge a conceptual gap in the body of literature. While this study conducted extensive analysis, this is the first iteration of the GSC framework and further study is required to examine its potential application to multiple and varied case studies.

Further study of cyber technologies and their impact on the international system is warranted and this research could be utilized as a foundation to examine related topics.

For instance, while this paper did not address the growing concern of cybercrime, a future study could examine the cases of states who commit cybercrimes for financial gain. It is not common for states to participate in cybercrime, normally individuals or small groups commit cybercrimes, such as identity theft, ransomware attacks, or any other computer crime for financial gain. North Korea for example, is frequently conducting cybercrimes to help counter international sanctions and fund their weapons program. Scholars could also build upon this research to examine what role global environmental policy and climate change will have on the world's internet network systems. As sea levels rise and major weather events become increasingly common and destructive, the impact to global networks could be catastrophic without a plan. Additionally, this research could serve as a foundation for further study of ICTs and their role in advancing foreign and domestic agendas of states.

The internet and related technologies have altered the traditional power structures in the international system and created a new opportunity for states in cyberspace. ICTs are more than a independent variable and this research has shown the significance in including them as integral parts to the international system. Cyber technology is constantly changing, new vulnerabilities are being discovered, and new methods of warfare are being developed and for that reason, cyber studies in international relations will have plenty of research opportunities now that the game has changed.

References

- Alsabah, N. (2016). *Information Control 2.0: The Cyberspace Administration of China tames the internet*. Mercator Institute for China Studies. Retrieved from https://www.merics.org/sites/default/files/2019-08/MERICS_China_Monitor_32_Eng.pdf
- Anderson, C., & Sadjadpour, K. (2018). *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Washington, DC: Carnegie Endowment for International Peace.
- Barnett, M., & Duvall, R. (2005). Power in global governance. In M. Barnett, & R. Duvall, *Power in Global Governance* (pp. 1-32). Cambridge: Cambridge University Press. doi:<https://doi.org/10.1017/CBO9780511491207>
- Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8(2), 121-144. doi:10.1111/ips.12048
- Bednarz, A. (2019, August 5). Evolution of the internet: Celebrating 50 years since Arpanet. *Network World*. Retrieved from <https://www.networkworld.com/article/3410588/evolution-of-the-internet-celebrating-50-years-since-arpanet.html>
- Bennett, A., & Elman, C. (2007). Case Study Methods in the International Relations Subfield. *Comparative Political Studies*, 40(2), 170-195. doi:10.1177/0010414006296346
- Bowles, A. (2006). The changing face of the RuNet. *Control+ Shift. Public and private usages of the Russian Internet*, 21-33.
- Brown, M., Daly, N., & Moss, B. (2018, June 4). *Companies Will Feel The Weight Of Team Telecom Oversight*. Retrieved from Wiley: <https://www.wiley.law/article-Companies-Will-Feel-The-Weight-Of-Team-Telecom-Oversight>
- Buchan, B. (2002). Explaining war and peace: Kant and liberal IR theory. *Alternatives: Global, Local, Political*, 27(4), 407-428. doi:10.1177/030437540202700401
- Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese-Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594-613. doi:10.1177/1367549417751151

- Bureau of Industry and Security. (2019, May 15). *Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List*. Retrieved from U.S. Department of Commerce: <https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd>
- Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium: Journal of International Studies*, 43(2), 640-659. doi:10.1177/0305829814562655
- Carr, M. (2016). International Relations Meets Technology Theory. In M. Carr, *US Power and the Internet in International Relations: The Irony of the Information Age* (pp. 16-44). Palgrave Macmillan.
- CCDCOE. (2015). *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?* Retrieved from The NATO Cooperative Cyber Defence Centre of Excellence: <https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/>
- CCDCOE. (2020). *About US*. Retrieved from NATO Cooperative Cyber Defence Center of Excellence: <https://ccdcoe.org/about-us/>
- Christou, G., & Simpson, S. (2007). Gaining a Stake in Global Internet Governance. *European Journal of Communication*, 22(2), 147-164.
- Cooper, M. (2018). 5G Technology Briefing. *ITNOW*, 60(3), 16-20. doi:10.1093/itnow/bwy062
- Cox, J. (2015, July 6). *The FBI Spent \$775K on Hacking Team's Spy Tools Since 2011*. Retrieved from WIRED: <https://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/>
- Croxton, D. (1999). The Peace of Westphalia of 1648 and the Origins of Sovereignty. *The International History Review*, 21(3), 569-852. Retrieved from www.jstor.org/stable/40109077
- Cylance. (2014). *Operation Cleaver*. Cylance. Retrieved from https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf
- Davis, J. (2007, August 21). *Hackers Take Down the Most Wired Country in Europe*. Retrieved from WIRED: <https://www.wired.com/2007/08/ff-estonia/>

- Donahue, T. (2020). The Worst Possible Day: U.S. Telecommunications and Huawei. *Prism : A Journal of the Center for Complex Operations*, 8(3), 14-35.
- Drefuss, B., & Dreyfuss, E. (2013, June 7). *What is the NSA's PRISM program? (FAQ)*. Retrieved from c/net: <https://www.cnet.com/news/what-is-the-nsas-prism-program-faq/>
- Eeten, M. J., & Mueller, M. (2012). Where is the governance in Internet governance? *New Media & Society*, 15(5), 720-736. doi:10.1177/1461444812462850
- Epifanova, A. (2020). Deciphering Russia's "Sovereign Internet Law": Tightening Control and Accelerating the Splinternet. *German Council on Foreign Relations (DGAP)*. Retrieved from <https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law>
- Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*, 27(3), 221-244. doi:10.1177/0192512106064462
- Field, M., Chowdhury, H., & Sanchez, R. (2019, October 30). *Israel's NSO: The shadowy firm behind the 'chilling' spyware used to hack WhatsApp and cloud services*. Retrieved from The Telegraph: <https://www.telegraph.co.uk/technology/2019/05/14/israels-nso-shadowy-firm-behind-chilling-spyware-used-hack-whatsapp/>
- FlorCruz, J. A., & Seu, L. (2014, April 23). *From snail mail to 4G, China celebrates 20 years of Internet connectivity*. Retrieved from CNN: <https://www.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html>
- Franceschi-Bicchierai, L. (2014, April 22). *NSA Finally Reveals How PRISM Works, But It's Nothing New*. Retrieved from Mashable: <https://mashable.com/2014/04/22/nsa-prism-report/>
- Franceschi-Bicchierai, L. (2014, June 5). *The 10 Biggest Revelations From Edward Snowden's Leaks*. Retrieved from Mashable: <https://mashable.com/2014/06/05/edward-snowden-revelations/>

- Franceschi-Bicchierai, L., & Cox, J. (2018, September 20). *They Got 'Everything': Inside a Demo of NSO Group's Powerful iPhone Malware*. Retrieved from Vice: https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo
- Gao, J. (2013, October 3). Internet Public Opinion Analyst. *The Beijing News*. Retrieved from http://epaper.bjnews.com.cn/html/2013-10/03/content_469152.htm?div=-1
- Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2), 41-73. doi:10.1162/ISEC_a_00136
- Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *LAW, INNOVATION AND TECHNOLOGY*, 9(2), 159-189. doi:10.1080/17579961.2017.1377914
- Harris, M. (2020, February 6). Google and Facebook turn their backs on undersea cable to China. *TechCrunch*. Retrieved from <https://techcrunch.com/2020/02/06/google-and-facebook-turn-their-backs-on-undersea-cable-to-china/>
- Hobbes, T. (1929). *Leviathan (Reprint ed, 1651)*. London: Oxford University Press. Retrieved from https://heinonline-org.jpallnet.sfsu.edu/HOL/Page?collection=beal&handle=hein.cow/hobbe0001&id=2&men_tab=srchresults
- Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: finding the governance in Internet governance. *New Media & Society*, 19(9), 1406-1423. doi:10.1177/1461444816639975
- Human Rights Watch. (2000). *The Suppression of the China Democratic Party*. Human Rights Watch. Retrieved from <https://www.hrw.org/report/2000/09/01/china-nipped-bud/suppression-china-democracy-party>
- Hynek, N. (2017). Regime Theory as IR Theory: Reflection on Three Waves of 'Isms'. *Central European Journal of International & Security Studies*, 11(1), 11-30.
- Internet Corporation for Assigned Names and Numbers. (2020). *About ICANN*. Retrieved from [icann.org: https://www.icann.org/resources/pages/welcome-2012-02-25-en](https://www.icann.org/resources/pages/welcome-2012-02-25-en)
- IT Advisory KPMG China. (2017). *Overview of China's Cybersecurity Law*. KPMG. Retrieved from <https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>

- Jensen, E. T. (2017). THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS. *Georgetown Journal of International Law*, 48(3), 735-778. Retrieved from <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf>
- Kadlecova, L. (2018). State Responsibility in the Cyber Age: The course towards Indirect Evidence. *Czech Journal of International Relations*, 53(4), 35-46. doi:<https://doi.org/10.32422/mv.1585>
- Kane, A. (2000). Reconstructing CULture in Historical Explanation: Narratives as CULtural Structure and Practice. *History and Theory*, 39(3), 311-330. Retrieved from <https://www.jstor.org/stable/2678014>
- Kello, L. (2013). The Meaning of the Cyber Revolution. *International Security*, 38(2), 7-40. doi:10.1162/ISEC_a_00138
- Koremenos, B., Lipson, C., & Snidal, D. (2004). *The rational design of international relations*. Cambridge: Cambridge University Press.
- Lewis, J. A. (2019, June 25). *Iran and Cyber Power*. Retrieved from Center for Strategic and International Studies: <https://www.csis.org/analysis/iran-and-cyber-power>
- Lukasik, S. J. (2011). Why the Arpanet Was Built. *IEEE Annals of the History of Computing*, 33(3), 4-21.
- Mačák, K. (2017). From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law*, 30, 877-99. doi:10.1017/S0922156517000358
- MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). *How does GCHQ's internet surveillance work?* Retrieved from The Guardian: <https://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work>
- Mahoney, J. (2000). Path dependence in historical sociology. *Theory and Society*, 29, 507-548.
- McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia*. Retrieved from BBC: <https://www.bbc.com/news/39655415>

- Mearsheimer, J. J. (2014). *The Tragedy of Great Power Politics* (Updated, E-book ed.). New York: W.W. Norton & Company.
- Miller, M. (2020, April 24). Lawmakers introduce legislation to boost American 5G efforts. *The Hill*. Retrieved from <https://thehill.com/policy/cybersecurity/494522-lawmakers-introduce-legislation-to-boost-american-5g-efforts>
- Moravcsik, A. (2014). Trust, but verify: The Transparency Revolution and Qualitative International Relations. *Security Studies*, 23, 663-688.
doi:10.1080/09636412.2014.970846
- Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, 19(6), 415-28. doi:10.1108/DPRG-05-2017-0025
- Nexon, D. H., & Wright, T. (2007). What's at Stake in the American Empire Debate. *American Political Science Review*, 101(2), 253-271.
doi:10.1017.S0003055407070220
- Nikkarila, J.-P., & Ristolainen, M. (2017). 'RuNet 2020' - Deploying Traditional Elements of Combat Power in Cyberspace? *2017 International Conference on Military Communications and Information Systems (ICMCIS)*, 1-8.
- NSA Special Source Operations. (2013). *NSA Prism Program slides*. The Guardian. Retrieved from <https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>
- Nye, J. S. (2009). Smart Power. *New Perspectives Quarterly*, 26(2), 7-9.
- Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. *Global Commission on Internet Governance Paper, Series 1*.
- Pagallo, U. (2015). Cyber Force and the Role of Sovereign States in Informational Warfare. *Philosophy & Technology*, 28(3), 407-425. doi:10.1007/s13347-014-0177-4
- Perlroth, N. (2019, February 18). *Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies*. Retrieved from The New York Times:
<https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html>

- PRC Information Office. (2010). *White Paper - The Internet in China*. The Information Office of the State Council of the People's Republic of China. Retrieved from <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Internet%20in%20China.pdf>
- Request for Special Temporary Authority, SCL LIC 20170421 00012; SCL-STA-20190906-00032; SCL-STA-2020_____ (Federal Communications Commission January 29, 2020).
- Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32. doi:10.1080/01402390.2011.608939
- Robinson, J. (2020, January 30). *Cyberwarfare statistics: A decade of geopolitical attacks*. Retrieved from Privacy Affairs: <https://www.privacyaffairs.com/geopolitical-attacks/>
- Ross, M. (2014). Understanding Interconnectivity of the Global Undersea Cable Communications Infrastructure and its Implications for International Cyber Security. *SAIS Review of International Affairs*, 34(1), 141-155. doi:10.1353/sais.2014.0014
- Rossokhovatsky, D., & Khvostunova, O. (2019, July 25). Why Russia Needs a "Sovereign Runet". *Institute of Modern Russia*. Retrieved from <https://imrussia.org/en/analysis/3029-why-russia-needs-a-%E2%80%9Csovereign-runet%E2%80%9D>
- Roth, A., & Priest, D. (2016, September 16). *Putin wants revenge and respect, and hacking the U.S. is his way of getting it*. Retrieved from The Washington Post: https://www.washingtonpost.com/world/europe/russian-hacking-a-question-of-revenge-and-respect/2016/09/15/8bcc8d7e-7511-11e6-9781-49e591781754_story.html
- Russia's Presidency in BRICS. (2015, October 22). *Nikolai Nikiforov: All of the BRICS Countries are Interested in IT Cooperation*. Retrieved from Official website of Russia's Presidency in BRICS: <http://en.brics2015.ru/news/20151022/582655.html>
- Sanger, D. E., & Perlroth, N. (2019, June 15). U.S. Escalates Online Attacks on Russia's Power Grid. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>

- Satariano, A. (2019, March 10). How the Internet Travels Across Oceans. *The New York Times*. Retrieved from <https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html>
- Schmitt, M. N. (2013). *Tallin Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.
- Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press. doi:10.1017/9781316822524
- Seawright, J. (2016). The Case for Selecting Cases That Are Deviant or Extreme on the Independent Variable. *Sociological Methods & Research*, 45(3), 493-525. doi:10.1177/0049124116643556
- Shackelford, S., & Alexander, F. (2018, January 12). China's cyber sovereignty: paper tiger or rising dragon? *Asia & The Pacific Policy Society*. Retrieved from <https://www.policyforum.net/chinas-cyber-sovereignty/>
- Shaji, R. S., & V. Sachin Dev, T. B. (2018). A methodological review on attack and defense strategies in cyber warfare. *Wireless Networks*, 3323-3334. doi:<https://doi.org/10.1007/s11276-018-1724-1>
- Shubber, K. (2013, June 24). *A simple guide to GCHQ's internet surveillance programme Tempora*. Retrieved from WIRED: <https://www.wired.co.uk/article/gchq-tempora-101>
- Snyder, Q. Z. (2013). Taking the System Seriously: Another Liberal Theory of International Relations. *International Studies Review*, 15, 539-561. doi:10.1111/misr.12069
- Starosielski, N. (2015). *The Undersea Network*. Durham: Duke University Press.
- Statista. (2019, May). *Revenue of major U.S. telecommunication service providers in 2018*. Retrieved from statista: <https://www.statista.com/statistics/201048/total-operating-revenues-of-us-telecommunication-providers/>
- Statista. (2020, March). *Number of internet users in China from December 2008 to March 2020*. Retrieved from statista: <https://www.statista.com/statistics/265140/number-of-internet-users-in-china/>

- Sydell, L. (2016, September 26). Republicans Say Obama Administration Is Giving Away The Internet. *NPR: All Things Considered*. Retrieved from <https://www.npr.org/sections/alltechconsidered/2016/09/26/495396014/republicans-say-obama-administration-is-giving-away-the-internet>
- TeleGeography. (2020). *Submarine Cable 101*. Retrieved from TeleGeography: https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions?__hstc=196094579.dd20c80ea2d9e1332aebb80b82eba14d.1584990610639.1584990610639.1584990610639.1&__hssc=196094579.1.1584990610640&__hsfp=1829511250
- The World Bank. (2018). *Individuals using the Internet (% of population) - Russian Federation*. Retrieved from The World Bank: <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2018&locations=RU&start=1995>
- UN GGE. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN Doc. A/70/174. Retrieved from <https://undocs.org/A/70/174>
- United Nations. (2020). *United Nations Department of Economic and Social Affairs*. Retrieved from un.org: <https://publicadministration.un.org/en/internetgovernance>
- University College London. (2019). *Professor Madeline Carr*. Retrieved from UCL: Professor Madeline Carr
- Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, 51(3), 347-360. doi:10.1177/0022343313518940
- Wakabayashi, D. (2020, January 16). *Google Reaches \$1 Trillion in Value, Even as It Faces New Tests*. Retrieved from The New York Times: <https://www.nytimes.com/2020/01/16/technology/google-trillion-dollar-market-cap.html>
- Waltz, K. N. (1959). *Man, the state, and war: a theoretical analysis*. New York: Colombia U.P.
- Warner, M. R. (2020, January 14). *Press Release: National Security Senators Introduce Bipartisan Legislation to Develop 5G Alternatives to Huawei*. Retrieved from

Mark R. Warner US Senator from the Commonwealth of Virginia:
<https://www.warner.senate.gov/public/index.cfm/2020/1/national-security-senators-introduce-bipartisan-legislation-to-develop-5g-alternatives-to-huawei>

Webb, M. C., & Krasner, S. D. (1989). Hegemonic Stability Theory: An Empirical Assessment. *Review of International Studies*, 15(2), 183-198.
 doi:10.1017/S0260210500112999

Xi, J. (2015, December 16). *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*. Retrieved from Ministry of Foreign Affairs of the People's Republic of China:
https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

Yi, S. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *China Political Science Review*, 2016(1), 81-93. doi:10.1007/s41111-016-0002-6