

REPORT DOCUMENTATION PAGE					<i>Form Approved</i> OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) 05/10/2019		2. REPORT TYPE Master's of Military Studies			3. DATES COVERED (From - To) SEP 2018 - APR 2019	
4. TITLE AND SUBTITLE Input the Title of your MMS, sample below: Cyber Sovereignty: The Assault on Human Rights				5a. CONTRACT NUMBER N/A		
				5b. GRANT NUMBER N/A		
				5c. PROGRAM ELEMENT NUMBER N/A		
6. AUTHOR(S) Maruska, Joseph, J, Major, USAF				5d. PROJECT NUMBER N/A		
				5e. TASK NUMBER N/A		
				5f. WORK UNIT NUMBER N/A		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068					8. PERFORMING ORGANIZATION REPORT NUMBER N/A	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)					10. SPONSOR/MONITOR'S ACRONYM(S) Dr. Matthew Flynn	
					11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT The creation of the Internet has changed how humans communicate and interact across the globe. The openness of the Internet stands in direct contradiction to that of sovereignty. Additionally, concerns in regards to the security of critical infrastructure or systems are a concern of states. Some states see the free access of information that is counter to their way of life unacceptable and have applied concepts of Westphalian Sovereignty to the Internet to the point of restricting human rights. To not fully support and prioritize human rights over state sovereignty is an alarming prospect that should be avoided if at all possible.						
15. SUBJECT TERMS Cyber Sovereignty, Human Rights, Internet, United Nations.						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON	
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College	
Unclass	Unclass	Unclass	UU	28	19b. TELEPHONE NUMBER (Include area code) (703) 784-3330 (Admin Office)	

*United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068*

MASTER OF MILITARY STUDIES

Cyber Sovereignty: The Assault on Human Rights

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Joseph Maruska

AY 2018-19

Mentor and Oral Defense Committee Member: MATTHEW ELYNN

Approved: _____

Date: _____

Oral Defense Committee Member: LICOR HARKOW

Approved: D.W. Harkow

Date: APRIL 25, 2019

Executive Summary

Title: Cyber Sovereignty: The Assault on Human Rights

Author: Major Joseph Maruska, United States Air Force

Thesis: Freedom of thought, religion, and speech are all values that hold high regard not only in the United States but in many places throughout the world. As states begin to isolate their populations from “questionable” content available over the Internet, freedom of speech and thought is manipulated and too often compromised. This denial should be overtly oppressed by the United States and international bodies such as the United Nations as the repression of human rights directly contradicts the Wilsonian ideals of the United States and the founding principles of the United Nations.

Discussion: The creation of the Internet has changed how humans communicate and interact across the globe. The openness of the Internet stands in direct contradiction to that of sovereignty. Additionally, concerns in regards to the security of critical infrastructure or systems are a concern of states. Some states see the free access of information that is counter to their way of life unacceptable. As such, states have applied concepts of Westphalian Sovereignty to the Internet by filtering what can be transmitted or received, surveilling their populations, and have come to the point of restricting human rights identified by the United Nations and codified in international law. Security measures can be implemented in a way that items such as key infrastructure and personal information can be protected without restricting human rights.

Conclusion: The United States helped shape and build the United Nations and develop international human rights into what they are today. To not fully support and prioritize human rights over state sovereignty is an alarming prospect that should be avoided if at all possible.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Table of Contents

	Page
EXECUTIVE SUMMARY	i
DISCLAIMER	ii
ACKNOWLEDGMENTS	iv
INTRODUCTION	1
SOVEREIGNTY	2
CHALLENGES TO SOVEREIGNTY	5
THE UNITED NATIONS AND HUMAN RIGHTS	7
ADVENT OF THE INTERNET	11
INTERNET EXPLOITATION AND VULNERABILITIES	12
CHINESE PERSPECTIVE	14
ADVOCACY FOR INTERNET FREEDOM	17
INTERNET FRAGMENTATION	19
INTERNET REGULATION	20
CONCLUSION	22
NOTES	24
BIBLIOGRAPHY	27

Acknowledgments

Thank you to Dr. Matthew Flynn, Dr. Jill Goldenziel, and LtCol Donald Harlow for their mentorship and guidance throughout the writing of this paper. Their support was instrumental in the completion of this milestone in my education.

A special thanks to my amazing wife Anna for allowing me to pursue my professional endeavors by caring for our three children and maintaining her active duty military career while I was away for most of a year expanding my knowledge and leadership capabilities. I could not have completed this program without her support.

INTRODUCTION

With the introduction of the modern Internet to the general population in the late 1980s, the world has become much smaller and increasingly interconnected. The idea of a platform where ideas could be exchanged without government interference was something unlike the world had seen and drastically changed business, communication, and society as a whole. The idea of state sovereignty, however, consisting of borders, restrictions to entry, and national laws and regulations threatened this freedom online. As time progressed and interconnectivity increased, some nations began, and continue to, apply sovereign-like rules to the Internet, a system that was not intended to have borders. Additionally, freedom of thought, religion, and speech are all values that hold high regard not only in the United States but in many places throughout the world. As nations hostile to this quality of openness online begin to isolate their populations from “questionable” content available over the Internet, freedom of speech and thought is manipulated and too often compromised. This denial of information goes against the Wilsonian ideals of United States foreign policy and is detrimental to the spread of the United States way of life. The world should not fear the Internet from the standpoint of the exchange of information, but states should realize the dangers of exploitation and take appropriate steps to safeguard critical systems upon which their population relies. Once this balance is attained, it is in the interest of western society to advocate for and support an open and free Internet across the world, through which a western standard would be more universally appreciated, and not viewed as tenets or guidelines of a single cultural. The end state is an open system that would test the nationalism of modern society and push through to a degree of human development and interconnectedness never before seen. All made possible through cyberspace.

In order to support the idea that it is for the greater good of the world to have a free and open Internet, this analysis looks at the background of sovereignty beginning with the Treaty of Westphalia and discusses the idea of sovereign equality, non-intervention, international norms and laws, and the current international state system. Challenges to sovereignty will then be discussed. Additionally, basic human rights will be assessed and discussed in regards to international law and norms through which disconnects between expected freedoms and actual freedoms will be shown. State sovereignty will then be compared to that of cyber sovereignty in regards to what it is, how state and cyber sovereignty differ, how the ideals of the initial development of the Internet contradict the ideals of state sovereignty. The complexities of an open system created by connections between physical devices within multiple sovereign states and vulnerabilities and potential exploitation will then be discussed. Next, a discussion in regards to the cost of allowing sovereign nations to isolate their population and the harm that comes from the suppression of information will be presented in followed by a reinforcement of the need for a proactive approach to pursue international freedom of information. Upon completion, the idea that human rights exceed those of a state's sovereignty will be reinforced. Additionally, it will be shown that security of key infrastructure and institutions can be accomplished without overarching government control of information which has the potential to usurp the international institutions that are in place and uphold human rights.

SOVEREIGNTY

Lassa Oppenheim, a German jurist and early proponent of international law, noted that sovereignty has had many definitions which have shifted over time and has never been defined in a way that has been universally agreed upon.¹ Sovereignty can be viewed as serving two major

purposes: first to rule or control those within in the confines of the state; and second, to protect the state's population from threats outside of the state.² In other words, sovereignty is seen as the right of a state to govern itself as it saw fit without interference or intervention from other states.

Many westerners see the Treaty of Westphalia in 1648 as the underpinnings of today's international structure in regards to state sovereignty, borders, international relations, treaties, and agreements. The peace that followed legitimized the ability for a state's ruler to govern their population without external interference.³ Westphalia marked a transition from a hierarchy state system to one of equality, where the individual states were seen as equals, not all subservient to an emperor or the Pope.⁴ As time passed, equality was also seen as extending to the individual within a state. Emerich de Vattel, an international lawyer most notably known for authoring *The Law of Nations*, a cornerstone to the development of modern international law, referred to equality as a natural right that extended beyond that of the state. He proposed that communities or states existed prior to international law, and their legitimacy is not a result of the law. Additionally, those states have an inherent right to freedom and equality unlikely to be surrendered. Finally, Vattel believed states were worthy of equality because their populations share the inherent right of equality as well.⁵ True state equality is seen as no state holding authority over other states, and the only true authority is international law. This Westphalian view dictates much of what is brought forward by statesmen today regarding cyberspace when addressing sovereignty in the cyber domain.

Besides customary international law, states are only bound to the international conventions that those states expressly recognize.⁶ As such, states may have different interpretations of what should or should not be seen as international law.⁷ A recent example

derives from the codification of customary international law stating the territorial waters of a state extends twelve nautical miles from the coast of a state into a body of water. Countries such as Libya have contended that they actually have ownership over a much larger territorial extension from their land mass. In 1973, Libya claimed the entirety of the Gulf of Sidra as its territory, extending territorial waters to as much as 140 nautical miles from the internationally recognized coastline, roughly twelve times the limit recognized by international law.⁸ In this sense, western reliance on a legal understanding of maritime boundaries causes friction with other nations and the international community. A more malleable view of law may be needed in cyberspace to achieve a higher level of international agreement and cohesion.

Alongside equality, the next major tenet of Westphalian peace was that of non-intervention. Non-intervention or non-interference norms are what allows the state to act as it will within the confines of its territory without interference from the outside world and was a recognized tenet of Westphalian sovereignty.⁹ Non-interference is what would be considered the essence of sovereignty in that a state cannot truly be sovereign if other parties are influencing or impacting its internal affairs.¹⁰ That being said, even in the eighteenth century, while the principle of non-intervention was standard practice, Vattel noted that if there was an internal rebellion within a state and that rebellion reached the level of civil war, outside states could intervene on behalf of the just party.¹¹ This contradiction to norms shows that the idea of non-intervention is not absolute. There are many examples of intervention within a sovereign state throughout history and the current international system via the United Nations (UN) explicitly allows for and facilitates intervention, which will be discussed in greater detail later in this analysis.

CHALLENGES TO SOVEREIGNTY

As the world has become more interconnected, an idea of effective sovereignty has emerged. Effective sovereignty is the idea that sovereignty is not strictly limited to that of geographic boundaries, but embodies a much larger idea. For instance, states can hold influence across the globe so that currencies, such as the United States dollar and Euro are not specifically restricted to a single nation, citizens hold multiple citizenships, commodities trade internationally, and the information is exchanged across global information networks.¹² These examples of effective sovereignty all stand in the face of traditional Westphalian sovereignty in that states very much have an influence upon the internal workings of other sovereign states through indirect means due to the nature of an increasingly interconnected world.

In addition to effective sovereignty, the international recognition of human rights also presents a direct contradiction to the non-intervention tenet of Westphalian sovereignty. It is important to note that for the first few centuries post-Westphalia, there was little concern for the responsibilities of a sovereign state in regards to its population. The idea that a state could essentially do what it wanted within the confines of its borders with and to its population without concern of interference was the norm. However, post-World War I, thinking changed, and the consideration of human rights began being included in the international understanding of sovereignty, that a state has a responsibility to its citizens.¹³ The concept that a state had the authority to do whatever it wanted to citizens within their borders was no longer an acceptable practice. The International Labor Organization established conventions that concerned work-related issues such as health and safety standards and were the first examples of an attempt to establish some form of international human rights. These conventions were not mandatory, but states could at their discretion, endorse them.¹⁴

A precursor to the peace negotiations of World War I was Woodrow Wilson's Fourteen Points. The Fourteen Points were the embodiment of what would later be known as Wilsonianism, which Henry Kissinger described as the driver of American foreign policy since its inception during the Wilson presidency.¹⁵ Wilson thought that the international role of America should be to promote the spread of its principles throughout the world. The concept being that like-minded states, specifically democratic societies, will not have reason to go to war with one another and as a result, international peace can be obtained.¹⁶ The Fourteen Points were used as a basis for the terms of peace following World War I and in turn laid the foundation for an international order based on universal law, self-determination, and opposed the idea of non-intervention.¹⁷ This became the basis for the League of Nations and indirectly later the United Nations (UN).¹⁸

Prior to Wilsonianism, Europe operated through balance of power politics, in that conflict between European states would typically end in one of two ways. The first that one state could become powerful enough to create an empire, the other that no individual state becomes powerful enough to impose its will on the others. Ideally, states would band together to stop an aggressor in an effort to balance power, or the status quo is such that no individual state will want to try and upset the international order.¹⁹ America operated unimpeded by the European employment of balance of power and likely benefited from the world order as America had no real geographic threats or competition. However, World War I brought the effects of balance of power politics directly to the American people. Wilson did not see balance of power politics as a way to maintain stable international relations, he saw peace as being possible through collective security and international law, which would need to be governed by an international institution.²⁰

As such, Wilson laid out his Fourteen Points in hopes to create a new international standard for state relations.²¹

While key tenets of Wilsonianism align with the current international system, Westphalian sovereignty, and the UN, the idea of non-intervention has been proven flexible throughout history. Trade sanctions, interstate conflict short of war, and the advent of Responsibility to Protect are just a few examples of breaches of sovereignty that have been accepted by the international community. The establishment of the International Criminal Court and the International Court of Justice established the framework for an international law system that can hold trials for states or individuals. Additionally, international law, standards, and norms have been established for the conduct of states and individuals beginning with the Universal Declaration of Human Rights (UDHR).

THE UNITED NATIONS AND HUMAN RIGHTS

In 1945, following World War II, the UN was founded based on the idea within the international community of “promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion.”²² In 1948, the UDHR was adopted by the UN. The UDHR clearly defined thirty specific articles seen as fundamental human rights that are to be universally protected and stated in clear terms that human life has worth and dignity.²³

The UDHR embodies the core beliefs upon which the UN was founded. Of note are the following articles and in particular relevance to the Internet is Article Nineteen:

Article One: All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article Two: Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

Article Eighteen: Everyone has the right to freedom of thought, conscience, and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship, and observance.

Article Nineteen: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The rights contained in the UDHR are quite similar to rights and protections afforded to United States citizens by United States law. Interestingly, the declaration has specific highlights stating that the rights are applicable to all people regardless of the sovereignty they are under. It goes on to say that they should be afforded freedom of thought, religion, expression, opinion, and the ability to seek, receive, and spread information via any media. As such, restrictions placed upon individuals by sovereign states, such as Internet censorship in North Korea, China, and Russia, are a direct contradiction to the ideals that are espoused by the UDHR.

However, the UDHR is merely a declaration and not international law, meaning it is a recommendation or a document of intent, but is not legally binding, even to signatory countries.²⁴ While the UDHR is not law, it was the basis upon which the 1966 International

Covenant on Economic, Social, and Cultural Rights (ICESCR) and the International Covenant on Civil and Political Rights (ICCPR) were founded.²⁵ The ICESCR and ICCPR are both codified in international law and set the baseline for recognized human rights across the globe.

Human rights law had arrived, but there was a realization that these rights would only be upheld by nations or leaders that wanted to uphold them, as sovereign states are afforded the jurisdiction to govern without external interference. Non-interference was also codified in Article 2.7 of the UN Charter which says states have an obligation to respect the sovereignty of other states and to not intervene in their internal affairs. Intervening in a state's internal affairs is seen as a violation of sovereignty and said state has the right to defend itself.²⁶

The International Court of Justice is the international means of holding a state responsible for international law violations, but is no more than a glorified arbiter between consenting states, meaning that both states must agree to the decisions and that the court has no power to enforce its rulings. Additionally, the International Court of Justice will not hear cases from individuals against a state; it is specifically restricted to grievances from states.²⁷ Essentially, without consensual agreement between states or a resolution from the UN security council for action, it is difficult to hold a state accountable for transgressions of international law. The International Criminal Court, established by the Rome Statute in 2002, allows individuals to be tried for the following four crimes: genocide, crimes against humanity, war crimes, and crimes of aggression.²⁸ These crimes are severe in regards to the violation of human rights. As such, the International Criminal Court is not a suitable court to hold individuals responsible for restricting human rights such as freedom of thought or religion.

Additionally, in 2001, the International Commission on Intervention and State Sovereignty (ICISS) released a paper titled, "Responsibility to Protect." The concept here is that

sovereign states have three primary responsibilities to their population within their state: the responsibility to prevent atrocities before they start by addressing root causes; the responsibility to react if or when an atrocity occurs with an appropriate response ranging from political, prosecutorial, and in extreme cases militarily; the responsibility is to rebuild and repair any damage done while addressing the cause and attempting to prevent a future occurrence. In concept, if a state is unable to uphold the responsibilities and protect its population, it forfeits its right to non-intervention and the international community has a responsibility to step in and correct the matter.²⁹ In 2005, the UN World Summit recognized the ICISS Responsibility to Protect report and incorporated portions into its outcome document. While not law, it establishes a method for the UN Security Council to intervene when a state is not protecting its population from genocide, war crimes, ethnic cleansing, and crimes against humanity.³⁰ The Responsibility to Protect has been invoked once by the UN Security Council in 2011 in response to the Libyan leader Colonel Muammar Qaddafi and his violent response toward large-scale anti-regime protests within Libya.³¹ In a similar situation, the UN Human Rights Council investigated the Syrian civil war and determined that the Syrian leader Bashar Al-Assad had committed multiple crimes against humanity and highlighted a need for international action. Unfortunately, the UN security council was unable to pass a resolution to intervene in Syria due to both Russia and China vetoing the security council resolution preventing a unified UN effort to effectively stop the violations.³²

While the Responsibility to Protect only applies in what would be considered extreme circumstances to prevent atrocities, it is an example of the international community having justification to violate a state's sovereignty. This shows, at least in regards to atrocity crimes, the

international community, in particular, the UN, believe there are times when sovereignty does not supersede the rights of individuals within the state.

ADVENT OF THE INTERNET

The advent of the Internet in the 1980s changed the way people could interact and share information instantaneously across the globe. Developed after the Cold War, the Internet was seen through an optimistic lens of western culture in that the world agreed with a globalized vision of shared information, knowledge, and western societal norms. Post-World War II, the United States saw little resistance internationally in its implementation of western ideologies and in the mid-1990s even China and Russia went along with this western international system.³³ Both are now seen by the United States as competitors in the international geopolitical system. However, since this was the international norm at the time, it was assumed throughout the development and implementation of the Internet, that western norms, values, and political systems would also propagate freely throughout this new medium of communication.³⁴

Initially, the Internet's design was challenged by maintaining reliable connections and enhancing the actual technology and capabilities, not so much by security. The networks were originally used for sharing of information between universities at a relatively small scale with minimal connectivity. Security was a much lower concern than the reliability of the system. Security was also inadvertently built into the initial implementation of the Internet in that the code used was so specific and fault intolerant that manipulation was difficult without bringing the system down. Essentially, exploiting early code was difficult.³⁵ Additionally, at the time, key infrastructure and high-value items were not connected to the network. This is in stark

contrast to present day Internet and networking in that most infrastructure, business, communication, and economic frameworks connect in some way to the Internet.

Throughout the 1990s as the Internet evolved further into commercial and public use, it took on the properties of a free domain—free meaning free of government control, free to share information and data, and open to all for access. The thought was the Internet domain was becoming so complex and widespread that no single entity could truly control it. The mindset of a safe, free, and democratic medium of communication was perpetuated in western culture. As such, there was a driving force to use this new tool in the private sector to enhance business and infrastructure.³⁶ The Internet was eventually opened to private carriers and as a result, the face and structure of the Internet were dramatically changed. Moving from an academic mindset to a commercial mindset required rapid evolution and implementation. As a direct result, new programming languages were developed which were more fault tolerant and easier to code in an effort to help speed up the process of writing computer code. Software companies also started releasing functioning programs, though potentially incomplete or unsecured, in order to make profits and stay afloat in the rapidly changing market.³⁷ While this made for ease of development and rapid release of the software, it also opened up new avenues of exploitation.

INTERNET EXPLOITATION AND VULNERABILITIES

The ideals that the Internet was founded upon quickly became leveraged by individuals looking to exploit the system that was in place. The belief that the Internet should be open, accessible, and free has begun to waiver even in democratic, capitalist states. The vast unregulated and relatively vulnerable Internet domain created opportunities for criminal organizations, governments, and even the average citizen to exploit data, personal information,

money, and gain political leverage points.³⁸ As governments began to realize there was a threat to their social, technical, and economic systems, they started building cyber borders, monitoring traffic in and out of their countries and in some cases blocking or restricting the flow of specific information.³⁹

The Internet rapidly began to expand into the “global commons” that it is today. In that, it is seen as a universally accessible communication medium.⁴⁰ As of October 2018, it is estimated that 3.7 billion people enjoy access to the Internet.⁴¹ As reliance on the Internet has increased so has the need to protect the vulnerabilities and key infrastructure. While a virtually interconnected world, there are physical elements in terms of the hardware and communication lines that facilitate the Internet. This infrastructure is located within the physical confines of states. As such, these physical manifestations within sovereign states can cause conflict in the global operation of the Internet through the implementation of state sovereignty.⁴² This requirement highlights the contradiction between a state’s sovereign right and the inherent open nature of the Internet.⁴³

In addition to control over key Internet infrastructure, states also have concerns about the openness of the Internet and the impact that quality can have on the local population and a state’s critical infrastructure. In regards to the local population, many states including China, Iran, and even the United States, have begun imposing filtering, restrictions, or monitoring of the data that enters and exits the sovereign confines of their state.⁴⁴ The United States in particular, via the Edward Snowden leaks of 2013, was shown to have a massive Internet surveillance operation run by the National Security Agency (NSA). The discovery of this covert campaign led to mistrust of the United States and a loss in its credibility and furthered desires by states to increase their cyber sovereignty.⁴⁵

A sovereign state does enjoy the right to protect itself from cyber threats. The United States Department of Defense (DoD) in its 2018 Cyber Strategy recognized the need for the United States to protect itself from cyber threats. The department identified a need to protect DoD networks, systems, and information, as well as the need to protect non-DoD equivalents in order to protect the interests and well-being of United States citizens from cyber threats.⁴⁶ As the Internet has matured, combined with the interconnectedness of infrastructure and industry, states have become well aware of the threats malicious actors can have to the livelihood of their citizens and society as a whole.⁴⁷

CHINESE PERSPECTIVE

In response to fears and legitimate impacts on social society from the Internet, many nations have begun implementing their own forms of cyber sovereignty. Retired Chinese Major General, now a senior advisor to the China International Institute for Strategic Society, General Hao Yeli describes the Internet and its underlying architecture as divided into three layers and provides recommendations on how she believes sovereignty should be handled at each level. The first layer is the foundational infrastructure upon which the Internet is built and allows for its operation. This layer ideally has a set of standards and is uniformly implemented across the globe in order to most efficiently operate the Internet. Standardization and uniformity would allow for ease of distribution and implementation across the globe. States should strive to interoperate as much as possible at the physical level.⁴⁸

The second level is the application level. This consists of Internet service providers and the integration of technologies that enable trade, the economy, or are incorporated in the everyday life of the citizen. Yeli claims that at this level, sovereignty should be flexible to meet

the needs of the local conditions in a balanced manner and to meet security needs and respect freedom.⁴⁹ The second level is where your typical business or end Internet user would reside, and the idea that some level of protection is needed seems like a reasonable conclusion. However, this is the level that is most impacted by China's state-imposed national firewall, a state-conducted effort to monitor, restrict, and control all information coming into and leaving the nation via cyberspace.

The third level is the core. The core consists of what Yeli describes as "regime, law, political security, and ideology, which is unchallengeable and includes the governing functions and embodies the core interests of the country." In her mind, these core functions cannot and shall not be infringed upon. She believes differences between cultures should be respected and tolerated.⁵⁰ This is a strong stance appeared to be aimed at democratic ideologies and insisting they not try to impose change on Chinese culture or their way of life via online access.

General Yeli's ideas for the operations and sovereign implications on the Internet appear reasonable. She highlights the contradiction between sovereignty and international human rights such as freedom of speech and thought.⁵¹ However, she later espouses that each country has natural jurisdictional power or sovereign right over the information transmitted by the state's infrastructure.⁵² A specific example is the extensive firewalls in China that were implemented in 1995. The goal of the firewalls was to "prevent unhealthy foreign influences from corrupting China's Internet users."⁵³ The implementation of Chinese Internet firewalls shows a direct contradiction between the openness desired by netizens and the position held by the Chinese government.

General Yeli also articulates the three main actors in cyberspace or on the Internet. The first is the citizen, also referred to as the netizen. At the individual level, Yeli indicates that their

freedoms are desired, but that governments need to impose regulations, boundaries, and laws for the safety and regulation of the Internet. The next actor is the state and its government, which is where additional contradictions occur. She is correct when she states the government seeks to further its agenda and goals. She then quotes Chinese President Xi Jinping as stating,

“Cyberspace is people-centered. We should make the Internet better benefit the people. The people on the Internet equal public opinions on the Internet. Our leading cadres go where the masses are; they must learn to follow the mass line through cyberspace and respond positively to the concerns and doubts of netizens.”

Yeli goes on to continue the contradiction describing the need to listen to the citizen and use their wisdom to guide democracy, values that are mirrored by the “ruling party.”⁵⁴

The third and final actor Yeli discusses is the international community, which has a desire to have an open and free exchange of information. She states this is in the interest of the world but notes the difference between the openness desired and that of a state’s sovereignty. She believes there can be a balance but is concerned by the advent of a globalized western culture intruding into Chinese space via online access.⁵⁵

Although Yeli does bring up a valid point in that to participate openly on the Internet, a state has to sacrifice some of its sovereignty, that sacrifice achieves a greater good in the global community through the exchange of ideas and culture, development, commerce, and security. She highlights the benefits to a single interconnected standardized Internet to facilitate these exchanges, but again warns against the push toward one global ideology or governance. This view explains China’s resistance to a free and open Internet within its borders, a fear of change to the ideology of their people.

Cyber sovereignty, best understood as the process of filtering data into and out of a state, is now the response to unwanted thought and fear by states such as China. In 2015, Xi Jinping stated that a nation has a right to regulate and develop their Internet, which infers that state boundaries would or should define cyber boundaries as well.⁵⁶ China’s cyber sovereignty

follows two basic principles. The first is to censor data from its citizens that the government feels would be harmful to the regime. The second is to change control or governance of the Internet from that of the private sector to that of an international organization such as the UN.⁵⁷ By 2016 China passed what it coined was its “Cyber Security” law. This law essentially increased the ability of the government to monitor, record, and stop the transmission of data deemed to be illegal by the state. Additional laws grant the Chinese government control over mandatory security guidelines and control over infrastructure and companies that the government sees as critical infrastructure. The goal stated by China for these mandates is to protect cyber sovereignty, citizen rights, and national security.⁵⁸

ADVOCACY FOR INTERNET FREEDOM

The United States has repeatedly been a strong proponent of Internet freedom. The State Department’s Global Internet Freedom Task Force was established in 2006 with the guiding principle of promoting Internet freedom and to denounce censorship. In 2010, Secretary of State Hilary Clinton stated that she believed that governments had no right to restrict an individual’s “freedom to connect” in regards to the Internet, information, and other individuals. Additionally, in 2011, Clinton stated that America was as committed to the protection of human rights online as it is offline.⁵⁹ In 2011, the United States established the Freedom Online Coalition with twenty-three other nations in order to promote a free and global Internet. Throughout the last decade, efforts have also been made to enhance Internet freedom via multiple United States government agencies in an effort to circumvent firewalls in foreign nations, enhancing user access to information, and preventing the monitoring of the population’s Internet usage by state actors. These agencies also made an effort to enhance existing Internet infrastructure and repair

or replace Internet connections globally.⁶⁰ The United States has also used diplomatic practices to promote Internet freedom and freedom of speech by pressuring oppressive regimes to release imprisoned bloggers. In 2012, the United States also supported a UN resolution affirming that human rights are to be respected not only offline but online.⁶¹

A common, connected, unrestricted Internet is what its founders intended and is what allows for not only a free society but an efficient well-running Internet. This is what is referred to as an open Internet. The original basis upon which the Internet was derived was that of an interconnected system in which any device was capable of exchanging data with any other device connected to the network that was willing to exchange data. The network consists of interconnected systems with common communications protocol and standards to ensure universal interoperability.⁶² Additionally, the connectivity and interoperability require a consistent seamless experience so all users can access all information from any location connected to the network. An interconnected, unimpeded, universal network is what would be considered an open Internet or an unfragmented Internet.⁶³

The United States has been a large supporter of individual Internet freedoms and for an openness to exchange information and ideas, that those ideas should not be cut short or infringed upon, particularly by state governments. Unfortunately, the American desire for a free and open system lost credibility and apparent sincerity with the 2013 Edward Snowden leaks. The leaks exposed that the National Security Agency (NSA) was conducting a mass surveillance program on the Internet.⁶⁴ The exposure hampered the United States' ability to rebuke efforts by states to have greater governmental control over the Internet. The UN also condemned the actions which were used by other states to push Internet privacy laws and protections for individuals on the Internet. It led to a questioning of the role the United States should play in the governance of the

Internet as well as compared that program to that of something the Chinese or Iranian governments would conduct.⁶⁵ This revelation not only lowered the trust of the United States government by the international community but increased questioning of how it should or should not be governed.

INTERNET FRAGMENTATION

The fear of spying, data compromise, intellectual property theft, and individual privacy concerns have led to a focus on security and regulation of the open Internet. These concerns have led to what would be considered the fragmentation of the Internet. Geoff Huston, the Chief Scientist at the Asia Pacific Network Information Centre (APNIC), defines Internet fragmentation as pressures on the network that create diverse outcomes which are no longer consistent or coherent.⁶⁶ Fragmentation of the Internet can be further divided into the categories of technical, governmental, and commercial. Technical fragmentation is the inability for the network to fully interoperate consistently to all endpoints. Governmental fragmentation consists of policies or actions that restrict the use of the Internet. Commercial fragmentation is a result of business practices that restrict the use of the Internet. All of these forms of fragmentation vary in regards to why they impact the operation of the Internet, but they all share commonalities in that they are considered intentional or unintentional and they can have positive or negative impacts not only on the Internet but on society.⁶⁷ Firewalls are an example that can be used as a very oppressive device such as how China uses it, or a useful component for securing digital resources from unwanted connections.⁶⁸ Additionally, private networks or proprietary connections are needed in some instances such as the banking or financial industry that requires a degree of stability and speed that the public Internet cannot replicate. Entities that require the exchange of

large volumes of data at high rates and consistent speeds may also utilize private connections segmented from the Internet.⁶⁹ These methods, while fragmenting the Internet, provide positive impacts while not negatively impacting users.

Increased public awareness and debate of the Snowden leaks were that of data localization, a form of governmental fragmentation in which user data is stored within the confines of a host state. The localized data has protections in order to safeguard as well as restrictions on what entities can access or manipulate said data.⁷⁰ Earlier catalysts for data localization comes from a desire to not be potentially dependent on, or vulnerable to, a foreign nation for the data necessary for critical infrastructure or financial institutions.⁷¹ An additional example of fragmentation is that of the Brazilian government and the European Union's plan of running a dedicated communications line between Brazil and Europe with the express purpose of routing traffic to avoid reliance on United States hubs.⁷² These kinds of actions absolutely affect the overall consistency and operation of the Internet. Overall, concerns from the cumulation of fragmentation activities will lead to an Internet in which depending on where the connection is made can affect what is able to be accessed or even transmitted. When thinking about completely isolated states such as North Korea, these ideas become even more troubling.

INTERNET REGULATION

How should the Internet be controlled or governed? The Global Commission on Internet Governance believes that there should be a singular Internet that is protected and accessible by all. Countries such as China and Russia believe a state has the right through sovereignty to control the Internet within the confines of their borders. Others believe it should be a coalition of private companies and organizations.⁷³ Regardless, as technology advances and companies or

governments implement controls over data and its exchange, the Internet becomes more and more fragmented.

From a security standpoint, there are definitely some benefits to be seen from various forms of fragmentation, all of which are forms of cyber sovereignty. The idea that the Internet and all data contained within could be free of any impediment is not realistic. The opportunity of exploitation leading to personal, corporate, and national losses is too great. The goal is and should continue to be a proper balance between security and an open Internet. This does not need to come at the cost of a loss of human rights. The restriction of speech and information from a population of people should not be acceptable in the international community.

There is a fine line between protection of infrastructure, banking institutions, industry, and personal data and the censorship or restriction of thought, opinion, and speech. As such, cyber sovereignty is very much in opposition to Wilsonian ideals. There are many instances in which restriction of rights is condemned within the international community, but states that impinge on human rights are still afforded the privileges of participation within the UN.

Additionally, the Westphalian concept of non-intervention is becoming a difficult standard to uphold in today's ever-connected world. As discussed, there are specific instances where the UN believes that the rights of the individual supersede that of the state. That a state has a right as a sovereign entity to protect the human rights of its people, and if unable to do so, it is the responsibility of other states to correct the state. In the case of responsibility to protect, this enables the potential use of military force to correct the situation. In regards to the suppression of human rights, it may be time to start increasing the negative repercussions from the UN and other nations in reaction to states acting in such a manner. The fact that the international community allows a state government, China, to only allow what it deems are

acceptable ideas, content, speech, religion, or expression to its population, which is roughly one fifth of the world's population, should be an incredibly frightening prospect, similar to oppressive regimes burning books to thwart dissenting opinions or ideas. It seems contradictory for an international governing body whose principles and framework are based on individual freedoms and human rights to continue to allow oppressive behavior from its member states. Yet, China is a permanent member of the UN Security Council. It is beyond time to strip international privileges granted by organizations such as the UN from states that do not abide by institutional standards.

CONCLUSION

A fine balance, or reasonable mix, can meet the needs of the netizen, the state, and the international community in regards to human rights, freedom, privacy, and security without impinging on them as well. In order to uphold and continue to support the Wilsonian ideals that the United States and United Nations were developed under, a serious look at the global free flow of information needs to be conducted. Additionally, the respect for human rights needs to exceed that of the respect for sovereignty and Westphalian derived non-intervention. Though the use of military force or the implementation of the responsibility to protect would be excessive and inappropriate, there are multiple avenues of political power individual states can take as well as international organizations in order to discourage the restriction of internationally recognized human rights. Overt and consistent messaging denouncing the restriction of human rights followed with directly attributable actions using all forms of political persuasion from sanctions to restricted privileges within the United Nations should be considered. Additionally, the United States needs to take a clear role in leading this effort within the international community by

sacrificing a portion of sovereignty to advocate for the greater good of international human rights that should not be infringed upon by a sovereign state. While Westphalian sovereignty is appropriate for ruling a population and promoting individual equality, its tenets of non-intervention are not compatible with the desired standards for the Internet.

Implicit in this alarm comes the question of what to do about actual and perceived cyber vulnerabilities. Some sacrifice is needed to safeguard infrastructure and sensitive data, but at the point at which laws change to restrict human rights in order to “protect” the population, it would appear at face value the desire of a governing body to control the thoughts of its people. A hasty reaction to a concern that will likely adapt before any legislative change can occur. The root of the issue is not the exchange of ideas, but the divisiveness and fear of a population that is easily exploited. Suppressing thought will further exacerbate a person’s ability to critically think and will perpetuate a cycle of distrust and misinformation. Any attempts to restrict human rights should be done so with caution particularly in an environment such as cyberspace that adapts and changes at a rate incomprehensible to that of bureaucracy. Authoritarian regimes are at the disadvantage in this battle, and to match their suppressive nature puts the legacy of the United States, the United Nations, and Wilsonianism at risk.

NOTES

-
- ¹ Luke Glanville, *Sovereignty & the Responsibility to Protect: A New History* (Chicago: The University of Chicago Press, 2014), 10.
- ² John Agnew, *Globalization & Sovereignty* (Lanham, MD: Rowman & Littlefield Publishers, Inc., 2009), 6.
- ³ Douglas Howland and Luise White, eds., *The State of Sovereignty: Territories, Laws, Populations* (Bloomington, IN: Indiana University Press, 2009), 3.
- ⁴ Gerry Simpson, *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order* (New York: Cambridge University Press, 2004), 30.
- ⁵ Simpson, *Great Powers and Outlaw States*, 32.
- ⁶ Statute of the International Court of Justice, Article 38, accessed May 9, 2019, <https://www.icj-cij.org/en/statute>.
- ⁷ Simpson, *Great Powers and Outlaw States*, 28.
- ⁸ Yehuda Z. Blum, "The Gulf of Sidra Incident," *The American Journal of International Law* 80, no. 3 (1986): 668-670.
- ⁹ Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999), 76.
- ¹⁰ Luke Glanville, *Sovereignty & the Responsibility to Protect: A New History* (Chicago: The University of Chicago Press, 2014), 13.
- ¹¹ Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999), 74.
- ¹² John Agnew, *Globalization & Sovereignty* (Lanham, MD: Rowman & Littlefield Publishers, Inc., 2009), 8.
- ¹³ Luke Glanville, *Sovereignty & the Responsibility to Protect: A New History* (Chicago: The University of Chicago Press, 2014), 12.
- ¹⁴ Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999), 110.
- ¹⁵ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 30.
- ¹⁶ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 30-33.
- ¹⁷ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 45.
- ¹⁸ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 54.
- ¹⁹ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 20-21.
- ²⁰ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 222.
- ²¹ Henry Kissinger, *Diplomacy* (New York: Simon & Schuster, 1994), 22.
- ²² International Commission on Intervention and State Sovereignty, *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty* (Ottawa, ON, Canada: International Development Research Center, 2001), 14.
- ²³ "Universal Declaration of Human Rights," December 10, 1948, *United Nations General Assembly Resolution 217 A*, 71.
- ²⁴ United Nations Educational, Scientific and Cultural Organization, "Social and Human Services: Declaration," accessed March 20, 2019, <http://www.unesco.org/new/en/social-and-human-sciences/themes/international-migration/glossary/declaration/>.
- ²⁵ International Commission on Intervention and State Sovereignty, *Responsibility to Protect*, 14.
- ²⁶ International Commission on Intervention and State Sovereignty, *Responsibility to Protect*, 12.

-
- ²⁷ International Court of Justice, *International Court of Justice Handbook* (Netherlands: The Hague, 2014), 5, <https://www.icj-cij.org/files/publications/handbook-of-the-court-en.pdf>.
- ²⁸ International Criminal Court, “How the Court Works,” accessed March 20, 2019, <https://www.icc-cpi.int/about/how-the-court-works>.
- ²⁹ International Commission on Intervention and State Sovereignty, *Responsibility to Protect*, XI.
- ³⁰ United Nations General Assembly, *A/RES/60/1: 2005 World Summit Outcome*. (New York, NY: United Nations, 2005), 30.
- ³¹ Anthony Bell and David Witter, *Escalation Intervention: Part 2*. (Washington, DC: Institute for the Study of War, 2011), 13.
- ³² Çağlar Açıkyıldız, “Failure to Protect in Syria: Will the UN Security Council Invoke R2P Ever Again?,” (Policy Brief No. 49, Global Political Trends Center (GPoT) Istanbul Kultur University, 2018), 26-27.
- ³³ Chris C. Demchak, “Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations of the cybered age,” *The Cyber Defense Review*, Vol. 1, No.1 (Spring 2016): 52.
- ³⁴ Demchak, “Uncivil and Post-Western,” 52.
- ³⁵ Demchak, “Uncivil and Post-Western,” 52.
- ³⁶ Demchak, “Uncivil and Post-Western,” 53.
- ³⁷ Demchak, “Uncivil and Post-Western,” 54.
- ³⁸ Demchak, “Uncivil and Post-Western,” 54.
- ³⁹ Chris C. Demchak and Peter Dombrowski, “Rise of a Cybered Westphalian Age,” *Strategic Studies Quarterly* (Spring 2011): 35.
- ⁴⁰ Wolff Heintschel von Heinegg, “Territorial Sovereignty and Neutrality in Cyberspace,” *International Law Studies: US Naval War College* Vol 89 (2013): 125.
- ⁴¹ Freedom House, *Freedom on the Net 2018* (Washington, DC: Freedom House, 2018), 11, https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.
- ⁴² Heintschel von Heinegg, “Territorial Sovereignty,” 125-126.
- ⁴³ Hao Yeli, “A Three-Perspective Theory of Cyber Sovereignty,” *Prism* Vol 7, No. 2 (2017): 114.
- ⁴⁴ Richard Fontaine, “Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in a Post-Snowden Era,” *Center for a New America Security* (September 2014): 3.
- ⁴⁵ Fontaine, “Bringing Liberty Online,” 3.
- ⁴⁶ United States Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC, 2018), 2, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
- ⁴⁷ Demchak and Dombrowski, “Rise of Cybered Westphalian,” 38-39.
- ⁴⁸ Yeli, “Three Perspective Theory,” 113.
- ⁴⁹ Yeli, “Three Perspective Theory,” 113.
- ⁵⁰ Yeli, “Three Perspective Theory,” 113-114.
- ⁵¹ Yeli, “Three Perspective Theory,” 110.
- ⁵² Yeli, “Three Perspective Theory,” 114.
- ⁵³ Jeremy Goldkorn, “The Chinese Internet: Unshared Destiny,” in *Shared Destiny*, ed. Geremie R Barmé, Linda Jaivin, Jeremy Goldkorn (ANU Press, 2015), 117.
- ⁵⁴ Yeli, “Three Perspective Theory,” 111.
- ⁵⁵ Yeli, “Three Perspective Theory,” 111-112.
- ⁵⁶ Emilio Iasiello, “China’s Cyber Initiatives Counter International Pressure,” *Journal of Strategic Security* 10, no. 1 (2017): 1.

-
- ⁵⁷ Niels Nagelhus Schia and Lars Gjesvik, *China's Cyber Sovereignty*, Policy Brief 2/2017 (Norwegian Institute of International Affairs, Feb 2017), 1, <https://www.jstor.org/stable/resrep07952>.
- ⁵⁸ Iasiello, "China's Cyber Initiatives," 6-7.
- ⁵⁹ Fontaine, "Bringing Liberty Online," 1-2.
- ⁶⁰ Fontaine, "Bringing Liberty Online," 2.
- ⁶¹ Fontaine, "Bringing Liberty Online," 2.
- ⁶² William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, *Internet Fragmentation: An Overview*, Future of the Internet Initiative White Paper (World Economic Forum, January 2016), 10.
- ⁶³ Drake, Cerf, and Kleinwächter, 10.
- ⁶⁴ Drake, Cerf, and Kleinwächter, 7.
- ⁶⁵ Fontaine, "Bringing Liberty Online," 3.
- ⁶⁶ Drake, Cerf, and Kleinwächter, 10.
- ⁶⁷ Drake, Cerf, and Kleinwächter, 4.
- ⁶⁸ Drake, Cerf, and Kleinwächter, 23.
- ⁶⁹ When two networks are better than one pg 128-129
- ⁷⁰ Drake, Cerf, and Kleinwächter, 41.
- ⁷¹ Drake, Cerf, and Kleinwächter, 42.
- ⁷² Fontaine, "Bringing Liberty Online," 4.
- ⁷³ Laura DeNardis, introduction to *The Shifting Geopolitics of Internet Access*, Global Commission on Internet Governance (Centre for International Governance Innovation, 2017), 2.

BIBLIOGRAPHY

- Açıkyıldız, Çağlar. "Failure to Protect in Syria: Will the UN Security Council Invoke R2P Ever Again?" Policy Brief No. 49. Global Political Trends Center (GPoT) Istanbul Kultur University, January 2018. <http://www.jstor.org.lomc.idm.oclc.org/stable/resrep14133>.
- Agnew, John. *Globalization & Sovereignty*. Lanham, MD: Rowman & Littlefield Publishers, Inc., 2009.
- Bell, Anthony, and David Witter. *Escalation Intervention: Part 2*. Washington, DC: Institute for the Study of War, 2011. <http://www.jstor.org.lomc.idm.oclc.org/stable/resrep07912.1>.
- Blum, Yehuda Z. "The Gulf of Sidra Incident." *The American Journal of International Law*, Vol. 80, No. 3 (1986): 668–677.
- Demchak, Chris C. "Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age." *The Cyber Defense Review*, Vol. 1, No.1 (Spring 2016): 49-74.
- Demchak, Chris C. and Peter Dombrowski. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (Spring 2011): 32-61.
- DeNardis, Laura. Introduction to *The Shifting Geopolitics of Internet Access*. Global Commission on Internet Governance. Centre for International Governance Innovation, 2017.
- Drake, William J., Cerf, Vinton G., and Kleinwächter, Wolfgang. *Internet Fragmentation: An Overview*. Future of the Internet Initiative White Paper. World Economic Forum, January 2016.
- Fontaine, Richard. "Bringing Liberty Online: Reenergizing the Internet Freedom Agenda in a Post-Snowden Era." *Center for a New America Security* (September 2014): 1-8.
- Freedom House. *Freedom on the Net 2018*. Washington, DC: Freedom House, 2018. https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.
- Glanville, Luke. *Sovereignty & the Responsibility to Protect: A New History*. Chicago: The University of Chicago Press, 2014.
- Goldkorn, Jeremy, "The Chinese Internet: Unshared Destiny." in *Shared Destiny*, 106-123. ed. Geremie R Barmé, Linda Jaivin, Jeremy Goldkorn. ANU Press, 2015.
- Heintschel von Heinegg, Wolff. "Territorial Sovereignty and Neutrality in Cyberspace." *International Law Studies: US Naval War College* Vol 89 (2013): 123-156.

- Howland, Douglas, and Luise White, eds. *The State of Sovereignty: Territories, Laws, Populations*. Bloomington, IN: Indiana University Press, 2009.
- Iasiello, Emilio. "China's Cyber Initiatives Counter International Pressure." *Journal of Strategic Security* 10, no. 1 (2017): 1-16.
- International Commission on Intervention and State Sovereignty. *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty*. Ottawa, ON, Canada: International Development Research Center, 2001.
- International Court of Justice, *International Court of Justice Handbook*. Netherlands: The Hague, 2014. <https://www.icj-cij.org/files/publications/handbook-of-the-court-en.pdf>.
- Kissinger, Henry. *Diplomacy*. New York: Simon & Schuster, 1994.
- Krasner, Stephen, D. *Sovereignty: Organized Hypocrisy*. Princeton, NJ: Princeton University Press. 1999.
- Schia, Niels Nagelhus and Gjesvik, Lars. *China's Cyber Sovereignty*. Policy Brief 2/2017. Norwegian Institute of International Affairs, Feb 2017. <https://www.jstor.org/stable/resrep07952>.
- Simpson, Gerry. *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order*. New York: Cambridge University Press, 2004.
- "Universal Declaration of Human Rights." December 10, 1948. *United Nations General Assembly Resolution 217 A*. 71-77, [http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217\(III\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/217(III)).
- United Nations General Assembly. *A/RES/60/1: 2005 World Summit Outcome*. New York, NY: United Nations, 2005. http://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_60_1.pdf.
- United States Department of Defense. *Summary: Department of Defense Cyber Strategy 2018*. Washington, DC, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
- Yeli, Hao. "A Three-Perspective Theory of Cyber Sovereignty." *Prism* Vol 7, No. 2 (2017): 109-115.