Webster
UNIVERSITY

Webster International Relations Review:
The Graduate Student Working Paper Series

2016

ISSN 2473-9502

http://www.library.webster.edu/wirr/

The 2015 United States-China Cyber Security Agreement and Its Impact on International Cyber Conduct

Aba Sasore[*]

[*] Ms. Aba Sasore, a 2016 graduate of Webster University's Master of Arts in International Relations program, acknowledges with thanks the assistance of Profs. Robert P. Barnidge, Jr., and David Reichardt and Ms. Linda Gardner. Email: abasasore35@webster.edu.

Abstract

On several different occasions, the United States has accused the People's Republic of China of hacking into or compromising information systems belonging to the United States or United States entities. In September 2015, the two countries adopted the Cybersecurity Agreement (Agreement) and since then have made notable progress in strengthening the Agreement. This paper explains why the United States entered into the Agreement with China. There seem to be three reasons for this. First, the United States used the Agreement as a framework to apply cyber norms in the international system. Many organizations and states have attempted to define cyber norms but have been unsuccessful in doing so. Second, the Agreement identified core cyber-related issues in order to achieve cooperation between "like-minded" and "other-minded" states. Last, the United States established behavioral limits on the private sector in order to protect United States interests. This paper uses the theoretical lens of regime theory to analyze the Agreement.

Keywords

China, United States, cyber security, information security, "like-minded," "other-minded," regime theory, bilateral agreement, Internet, cyberspace, United Nations, regime complex

Introduction

In September 2015, President of the United States Barack Obama and President of the People's Republic of China Xi Jinping jointly announced that the United States and China would begin working together to address problems and vulnerabilities associated with cyber security. Shortly thereafter, in December 2015, the United States Department of Homeland Security (DHS) and China's Ministry of Public Security began discussing the guidelines and the parameters of cooperation. In a 2015 joint public affairs press release, the United States Department of Justice (DOJ) and DHS explained the outcomes of the joint dialogue on cyber crime. The United States Attorney General and China's State Councilor agreed on mutual procedures for requesting and receiving assistance on cyber crime and other cyber malicious activities. In addition, the United States and China agreed to engage in a tabletop exercise in the spring of 2016 to ultimately "assess China's proposal for combatting terrorist misuse of technology . . . and to consider the United States' proposal on inviting network experts" (Joint Press Release 2015). The joint dialogue also requested both sides to collaborate with their respective agencies on issues related to intellectual property rights, such as the "theft of trade secrets, fraud and misuse of technology and communication for terrorist activities and network protection" (Joint Press Release 2015). The United States and China agreed to a second round of talks scheduled for June 2016, in Beijing.

The new partnership and dialogue come as a milestone in diplomacy mainly due to the United States' tense relationship with China on matters of cyber security. The *Washington Post* reported that Chinese hackers were allegedly responsible for hacking the information systems of the United States Office of Personnel Management (OPM) in early 2015, which resulted in the release of personal information belonging to thousands of United States Government employees (Nakashima 2015). OPM is responsible for human resource management across all federal agencies, including hiring, background services, and the management of retirement data. The security breach not only exposed security weaknesses in the United States Government's information security protection plan: it potentially placed thousands of Americans at risk to hostile foreign governments or rouge organizations. In May 2014, DOJ announced that five Chinese military officials would be charged with 31 counts of cyber espionage. Over a span of eight years, the DOJ investigation revealed that five Chinese military members hacked into the corporate computer systems of several United States companies and obtained proprietary intellectual property that could help advance China's economy.

Cyberspace serves as a public resource for people, governments, organizations, and businesses to interact with each other regardless of international borders, yet it has the potential to adversely impact cyber users. Cyberspace can facilitate illicit activities that inhibit economic growth, negatively impact everyday users, and impede the development of new technologies. Any one of these sources of illicit activities has the potential to compromise a nation's security and economic power. According to Moore's article "Cyber Attacks and the Beginnings of an International Cyber Treaty," countries frequently use cyber technology to conduct passive information gathering and offensive operations on other states. For example, "Estonia, a highly technological country, was brought to its knees by a series of attacks in 2007 that initiated in Russia and greatly disrupted Estonia's banking systems. Similarly, during the 2008 Georgia-Russian conflict, cyber attacks were used to shut down Georgia's banking and mobile phone systems" (Moore 2013:227). The shared nature of cyberspace is increasingly becoming associated with war-like terms such as "attack," "offensive," "defensive," "intelligence," and "operations." In this environment, illicit activities go beyond traditional military players, and combat-related actions can be carried out by civilian and state actors with increasingly advanced means and nefarious intent.

The diverse uses of the Internet adversely affect security for all cyber users, regardless of political boundaries, and challenge the smooth, collaborative functioning of an array of systems in the international community. This demonstrates the need for states to exercise their obligations to their citizens and for other international partners to seriously address issues of cyber security.

In light of previous cyber attacks on the United States attributed to China, why did the United States decide to negotiate the Cyber Security Agreement with China in September 2015? This research paper argues that the United States negotiated the Agreement with China to: 1) provide clarity on the application of cyber norms in the international system; 2) identify core security issues affecting states in order to sponsor collaboration between "like-minded" and "other-minded" states; and 3) establish behavioral limits on the private sector to protect the economic and national security concerns of the United States.

Literature Review

The following literature review covers scholarly works, the key international relations terms applied in this paper, the qualitative methodology used, and an explanation of the international relations theory that supports the thesis. It also extrapolates key concepts that assist in understanding international relations' role in cyber security. In addition, this section explains the qualitative process and questions that drive this research.

In "Cyber Attacks and the Beginning of an International Cyber Treaty," Moore states that "A cyber treaty may be a useful tool to step into the current void in customary international law, bridging the gap between state interests" (2013:228). Currently, customary international law regulates a state's actions in the international sphere, including situations of armed conflict and with respect to the use of force. Customary international law is reasonably clear in the kinetic arena, but it has not adequately accounted for cyber technology. Moore presents the arguments of a couple of scholars who believe that current customary international law is sufficient to regulate the use of cyber technology. Still, while "[c]ustomary international law may stave off such a flashpoint, but an international cyber treaty might prove beneficial by providing more clarity on acceptable international norms" (2013:230). Throughout his article, Moore identifies key limitations in customary international law and suggests how international treaty law might clarify the complex issues involved.

Customary international law does not define the notion of a cyber attack, which has left the definition of this concept open to interpretation. Unfortunately, scholars' definitions are often restrictive or omit key factors. Clarke's definition of cyber warfare in his book *Cyber War*, for example, primarily focuses on nation-states; it "excludes non-state actors as perpetrators and fails to distinguish cyber attacks from cyber crime or cyber war" (2013:233). Rule 30 of the 2013

Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) spells out a cyber attack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (2013:234). Moore argues that this definition limits the scope of cyber attacks to those with kinetic effect and fails to include cyber espionage and psychological cyber operations.

Given that customary international law does not specifically apply to cyber issues, Moore asks "whether the existing law applies to cyber issues at all, and, if so, how"; he focuses on *jus ad bellum* (the law related to the use of force) and *jus in bello* (the law of armed conflict). Can a cyber attack qualify as an armed attack? Cyber attacks certainly complicate the laws of war, in particular with respect to the principles of distinction, proportionality, and neutrality. States are required to distinguish between civilian objects and military objectives during their attacks in armed conflict, but because cyberspace has both civilians and military uses, the principle of distinction as applied to cyberspace raises a number of challenging questions (2013:234). The gravity of damage to civilian life or infrastructure is difficult to measure in a cyber attack as it "often has indirect, nonlethal or temporary effects" (2013:235). States are supposed to respect the rights of neutral states, but cyber attacks can be so pervasive that a cyber attack organized by one state can potentially involve the infrastructure of another state and thus violate the neutrality rule. As Moore points out, international law in this area needs to be clarified.

In "Cyber International Relations as an Integrated System," Vaishnav, Choucri, and Clark discuss how cyber has impacted traditional understandings of international relations. Essentially, cyber has caused a paradigm shift in the international relations system. The Internet, though operated by the private sector, benefits and affects actors across international borders and because of this has become a concern for non-governmental organizations, inter-governmental organizations, and international corporations. "The major actor that constitutes and defines International Relations – the State – is unable to control the cyber domain to any meaningful extent or to insulate itself from the implications of the new cyber realities" (2013:564). Cyber can give weaker actors an advantage over states with stronger relative power. Vaishnav, Choucri, and Clark acknowledge that there is very little literature on cyber international relations and spend the bulk of their research making the argument for a Cyber-IR system. Their work, which uses a design structure matrix, provides a useful conceptual framework but does not answer this paper's thesis question. It does a very thorough job of identifying the key players in cyber and their roles in the international system.

Hurwitz's article "The Play of States: Norms and Security in Cyberspace" discusses the collective actions that states have taken to develop norms and establish security for cyber. In a 2010 report, the United Nations Group of Governmental Experts (GGE) "recognized that private sector and civil society actors had roles to play [and were] assigned the dominant role in securing cyberspace to the states." From there, the GGE provided a "Code of Conduct" recommendation to the United Nations General Assembly. The Code of Conduct proposed that states should agree not to use "information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies" (2014:324).

Russia and liberal democracies had different reactions to the initial recommendations of the GGE. Russia responded with a draft treaty on cyber security; liberal democracies, in contrast, organized conferences in London (2011) and Budapest (2012) in response. The conferences were less concerned with the norms and security of cyber and more interested in facilitating Internet freedom. There were promising signs of a potential compromise between security and Internet freedom during the Seoul conference in 2013, which showed the fruits of Korean and Chinese work on cyber security through Computer Emergency Response Teams (CERTs).

A 2013 GGE report reaffirmed that international law applies to cyberspace but went on to contend that states have to determine exactly how the law applies to cyberspace. Hurwitz raises some of the same concerns that Moore does related to the law of armed conflict and the Tallinn Manual. Hurwitz's article identifies some of the problems that international organizations have with customary international law on cyber practices and suggests that agreements or treaties between states can compensate for the shortcomings of international law.

Jon Lindsay's "The Impact of China on Cybersecurity" introduces a table that typologies the cyberspace narrative. In it, Lindsay compares a cooperative political environment and competitive political environment against evolutionary and revolutionary technologies. He breaks the table into four quadrants:

1) Cooperative Political Environment and Evolutionary Technology – "Open Internet"
2) Cooperative Political Environment and Revolutionary Technology – "Cyber Security Norms"
3) Competitive Political Environment and Evolutionary Technology – "Contested Cyberspace"
4) Competitive Political Environment and Revolutionary Technology – "Cyber Warfare"

Lindsay's table provides a helpful analysis of the assumptions, threats, and counterarguments as relates to the United States and China.

While Western countries and China have differences of opinion regarding the openness of the Internet, they agree that it can spur on economic growth. However, whereas the "Western notion of cybersecurity emphasizes technical threats, China places greater weight on ideological threats" (2014:15). China is interested in securing information so that the Internet does not threaten its political legitimacy. Lindsay's article provides a detailed account and graphical data of the history of Chinese cyber hacking. "Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey observed that all 'nations on the face of the planet always conduct intelligence operations in all domains,' but 'China's particular niche in cyber has been theft and intellectual property'" (2014:26). The United States is concerned with the intent and purpose of actors in a contested cyberspace.

The United States and China understand that there is a military advantage involved in cyber warfare. Cyber provides an asymmetrical advantage to actors that can effectively exploit their capabilities. The Chinese have demonstrated an ability to conduct offensive attacks, but there is much debate as to whether China has the defensive capabilities to thwart a cyber attack.

Most of the research supports the argument that cooperation among states is necessary to address international cyber security. Lindsay's article helps break down what the United States and China deem as threats to cyberspace. The United States and China represent the two major schools of thought with respect to appropriate cyber security. Therefore, their ability to develop an agreement with each other will assist in fostering international cyber security norms generally.

Lifland's short article "Cyberwar" addresses the growing trend of cyber threats to the United States. The author discusses some of the steps that the United States has taken to secure cyberspace, including the President's "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" ("International Strategy for Cyberspace") and domestic legislation to secure the Internet. Lifland also addresses the differences between what states determine as a secure cyberspace. "Policies of the United States and the United Kingdom, want to be able to crack down on cybercrime without inhibiting the free flow of information between and within countries. In contrast, primarily promoted by Russia and China, states are concerned with limiting the flow of information across borders" (2012:7). "Cyberwar" provides a very clear picture of where the United States and China stand on the issue of cyber security but does not add more knowledge or depth than Moore's and Lindsay's articles.

The National Committee on American Foreign Policy's (NCAFP) policy document "Cyberpower and National Security" reviews cyber-related challenges and contains experts' recommendations as to how the United States should engage with cyber security. One expert recommendation, for example, urges a public-private partnership on cyber matters. "Like-minded" countries should work together on an international level and cooperate with such "other-minded" countries as "China and Russia, for example, on such issues of strategic importance as economic and industrial espionage. Since these are sensitive issues, seeking common ground on issues of mutual concern such as terrorism or cybercrime is important" (2012:6). Another expert recommendation addressed cyber as warfare and broke down the tactical, organizational, and strategic aspects of the fight against cyber attacks (2013:52). Yet another expert who contributed to the NCAFP policy document presented on Sino-American relations on cyber security (2012:54).

	Yes	No
Does customary international law address the issue of cyber security?	NCAFP (2013)	Moore (2013) Vaishnav, Choucri, and Clark (2013)
Are states responsible for securing cyberspace?	Hurwitz (2014) Moore (2013) Bajaj (2010) Henley (2014) Lifland (2012)	

Can a Sino-American partnership help secure cyberspace?	Lindsay (2015) NCAFP (2013)	
Can a Sino-American partnership on cyber security assist in creating international support for cyber security?	Lindsay (2015) NCAFP (2013) Moore (2013) Vaishnav, Choucri, and Clark (2013)	

Concepts

The following international relations concepts will be applied throughout this paper:

1) Diplomacy – an "official communication between states in efforts to arrive at an agreement on a particular issue or concern" (Sarkesian 2013:3).
2) Human Rights – "an extension of natural and inalienable rights. States have a duty to protect rights – if they fail to do this their sovereign status is in question" (Dunne and Hanson 2008:65). The paper acknowledges that the concept of human rights is interpreted differently by the United States and China.
3) Interdependence – "in world politics refers to situations characterized by reciprocal effects among countries or among actors in different countries" (Keohane and Nye 1977:8). Applying this concept assists in understanding the rationale behind the Agreement.
4) National Interest –the "expression of values projected into the domestic and international arenas" (Sarkesian 2013:6). The national interests of the United States are a core factor in the decisions that its officials make on cyber security.
5) National Security – "the ability of national institutions to prevent adversaries from using force to harm Americans or their national interests and the confidence of Americans in this capability" (Sarkesian 2013:2). This paper focuses on the national security interests of the United States.
6) Regime Complex – "a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages" (Nye 2014:7).

Theory

This paper applies an *international regime* theory of international relations to help explain the United States' decision to diplomatically engage with China on cyber security. Regime theory is a unique hybrid of international relations *structured realism* theory and neoliberalism. International relations scholars see international regime theory as a useful theory to address governance on the international stage (Karns and Mingst 2010:42). Krasner's definition of regime theory – "sets of implicit or explicit principles, norms, rules, and decision making procedures around which actors' expectations converge in a given issue area" (Karns and Mingst 2010:42) – has been widely adopted, including by this paper. According to Keohane's *After Hegemony*, explanations of principles, norms, rules, and decision-making procedures are key variables to our understanding of complex interactions leading to outcomes in the international arena (Majeski). "Principles are beliefs of fact causation and rectitude. Norms are standards of behavior defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice" (Gehring 1992:25).

Regime theory adopts structured realism's perspective on international actors and assumes that "actors in the international system are unitary and rational behaving units that act to promote their interests" (25). Regime theory accepts that international regimes were designed to advance the interests of hegemonic states. In addition, it accepts the economic neoliberalism concept of interdependence and assumes that actors will compromise on issues that ultimately promote their interests. Examples include trade, security, international law, and monetary systems (Bovcon 2013:7). Regime theory sees international law as a means to provide a formal framework allowing for specific provisions in international treaties and bilateral or multilateral agreements, as well as in considering informal norms and behaviors.

If accurately applied, regime theory would define cyber as an issue area, with the Agreement being addressed as a subset of cyber security. It is important to understand that regime theorists recognize cyber as an issue area without a regime. Their reasoning is that cyberspace is not governed; therefore, a regime complex would primarily manage its activities. A *regime complex* is "a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages" (Nye 2014:7). In other words, the regime complex pulls from a variety of institutions, regimes, and other rules in order to develop norms for an activity. Furthermore, within the cyber regime complex, there are sub-issues that may include human rights, crime, and intellectual property rights that the Agreement seeks to address; and in doing so, the Agreement contributes to the regime complex.

Methodology

This paper adopts a qualitative methodology based on such secondary sources as scholarly journals, press releases, and lecture notes. Peer-reviewed articles identify key concepts and address the main research question regarding cyber security in particular, namely why cyber security is so difficult to address in the international community. Additional research questions intended to operationalize the main research question are: 1) What is the significance of the United States' engaging China on cyber security?; 2) How does the Agreement further the United States' interest in cyberspace operations?; and 3) What impact does the Agreement have on other actors in the international community?

It is hoped that the research presented here provides insight as to how the United States will implement its new partnership with China. The scholarly literature helps explain the aims of the bilateral relationship, the goals it expects to address in international cyber security. This paper augments peer-reviewed articles with other serious authors working in policy institutions commonly known as "think tanks." Newspaper articles serve to characterize the narrative and shed contemporary perspective on cyber capabilities and concerns.

Establishing Cyber Security Norms

Article 38 of the Statute of the International Court of Justice defines customary international law as "evidence of a general practice accepted as law." States frequently use the United Nations as a diplomatic resource to create, implement, and regulate customary international law. A benefit of customary international law is its ability to clarify or define particular concepts or terms that affect nations throughout the world. However, customary international law is often left undefined and can be exploited by states for their own benefit, and at the expense of other actors in the international system. The emergence of cyber and its assortment of functions have posed a concern for the international community. According to Moore, Meyer, and Hurwitz, states have used cyberspace as a tool to conduct reconnaissance, attacks, and crimes against other states. The examples of cyber attacks over the last decade may signal a paradigm shift in the manner in which various actors conduct war-like operations. The growing debate among analysts and scholars is whether existing customary international law norms are sufficient to address cyber attacks. The core of this examination centers around two main issues: first, the fact that there is no universally accepted definition of a cyber attack; and second, the debate related to the application of the law of armed conflict to cyber attacks.

As Moore's "Cyber Attacks and the Beginnings of an International Cyber Treaty" argues, cyber capabilities have become extremely helpful to states in conducting military operations, but it should also be recognized that these capabilities are available to citizens across the globe. Currently, there is insufficient understanding of what is lawful in cyberspace and how responsibility is allocated in this arena. According to Moore, defining cyber attacks has been left to the interpretation of international relations scholars, who have been unable to agree upon a definition that is universally accepted by the international community. As a result, the term "cyber attack" is used interchangeably with such terms as "cyber espionage," "cyber war," and "cyber crime." Frequently, the definition leaves out key elements. Moore, for example, references Clarke's definition of cyber attack – an "unauthorized penetration by, on behalf of, or in support of, a government into another nations' computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls" (232-33) – and explains that this definition is limited in that it neither factors in non-state actors nor distinguishes between cyber attacks, cyber crime, and cyber war (if there is a difference) (233).

The Tallinn Manual was a unique attempt by the international community to define cyber attacks. The North Atlantic Treaty Organization (NATO) created a cyber defense wing to address issues surrounding cyber attacks and began a process that led to the adoption of the Tallinn Manual in 2013. Moore identifies an ambiguity in the Tallinn Manual's definition of cyber attacks with respect to the meaning of cyber operations, as well as the failure to specify if attacks are limited to kinetic action or extend to cyber espionage and psychological cyber operations (234).

International regime theorists would consider NATO a regime because the organization has set standards of behavior for a particular issue. NATO is generally involved in military action, and its interest in addressing cyber attacks through a cyber defense wing signals that perhaps cyber falls within the purview of the NATO regime. However, NATO's incomplete assessment of cyber attacks reveals that there are more components to cyber security than what NATO can contribute. Therefore, it is not sufficient for cyber security to solely belong to the NATO regime. States have also attempted to establish their own domestic definitions of cyber attacks. The United States Department of Defense, for example, defines a computer network attack as an "action taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" (Moore 2013:233).

It is reasonable to conclude that international cooperation between states and other actors is unlikely to clarify all aspects of cyber attacks in the near term. Still, the Agreement can provide an interim solution. The United States and China represent two of the most prominent cyber powers in the world today. Both nations understand the current scope of cyber technology and recognize the unchartered potential in cyber's capabilities. In light of this, the Agreement does not completely define a cyber attack, but it does provide insight into the types of operations against states that should not be tolerated. The Agreement focuses on the theft of intellectual property: the United States and China committed themselves to work together to address malicious cyber activity. Based on the Agreement, it appears that both countries consider cyber theft a form of cyber attack that must be defended against.

The absence of all-encompassing and universal definitions for cyber security-related terms has allowed the United States to project its own set of values onto the cyber regime complex that is the Agreement. "Regime analysts assumed that patterns of state action are influenced by norms, but that such norm-governed behavior was wholly consistent with the pursuit of national interests" (Haggard and Simmons 1987:492). The Agreement developed norms for cyber security, and in doing so, the United States as a state actor has been able to advance its own interests (as has China). The United States narrowed the Agreement to focus on concepts of crime, terrorism, and intellectual property theft and introduced these concepts as sub-issues of cyber, including them as components of cyber security. In essence, the United States welcomed a standard for cyber security that advocated for the cooperative prevention of information systems to be utilized to conduct crime, terror, and intellectual property theft on an international level.

Organizing "Like-Minded" and "Other-Minded" States

Cyber security is relevant to a wide variety of actors in the international system, but states have a unique responsibility to develop a consensus on international norms and standards for cyber conduct. The challenge for states is reaching an agreement that captures the perceived priorities in cyber security for "like-minded and "other-minded" states: in other words, creating an agreement that satisfies the varying perspective held by states. According to a review of the proceedings of a 2013 NCAFP-sponsored conference, "like-minded" countries are similar to the United States and include such democratic nations that encourage freedom of expression as Canada, the United Kingdom, and South Korea. In contrast, "other-minded" countries, such as

China and Russia, have alternative forms of government and are primarily concerned with information security within the context of cyber security. Several international organizations have created specialty subgroups to research, discuss, and design international norms on cyber security.

A United Nations-tasked group was pivotal to the identification of universal issues within international cyber security and the mobilization of countries. The GCE's 2010 report identified a number of concerns related to international security, in particular the use of malicious tools and methodologies by criminals, hackers, and state-sponsored entities in cyberspace (Hurwitz 2014:323). The GGE called upon states to "adopt confidence-building measures, exchange information on their respective national cybersecurity strategies and policies" (Hurwitz 2014:323). Regime theorists would argue that the regime complex facilitated the use of the GGE because it "permit[ted] the formation of clubs or smaller groupings of like-minded states that can pioneer the development of norms that may be extended to larger groups at a later time" (Nye 2014:9). States responded to the GGE's recommendations quickly and in various manners: the United Kingdom, for example, held a major conference in London in 2011, and the United States published its "International Strategy for Cyberspace" a year later. Each approach called upon states to work in unison on cyber-related issues, but it was clear that liberal democracies' cyber solutions and priorities differed greatly from the agendas of other states.

Russia and China competed with the United Kingdom's initiative in London by lodging recommendations with the General Assembly on international cyber norms, highlighting the international community's conflicting priorities on cyber security. The Sino-Russian proposal emphasized information security and worried that cyber, if left unregulated, could threaten the political legitimacy of nations. Liberal democracies rejected this proposal on human rights grounds and made Internet openness the focus of the 2011 London conference and the 2012 Budapest conference. "Western countries tend to consider it [cyber security] as a matter of maintaining an open and secure Internet without constraint on content. China and Russia, in contrast, consider content as a key element of the information space they wish to safeguard" (Meyer 2015:52). The Sino-Russian proposal distracted states from the original purpose of both conferences, as they "paid little attention to the norms for security and reliability" (Hurwitz 2014:324).

An important shift in cyber security norm development occurred during the 2013 Seoul conference, where South Korea demonstrated its ability to work with China through the East Asian CERT, a defense system designed to encourage coordination in order to protect critical infrastructure from cyber attacks. This partnership represents significant cooperation between "like-minded" and "other-minded" countries. The East Asian CERT reveals that achieving agreement between states with varying political agendas and perspectives on cyber security requires states to focus on cyber security sub-issues that affect them collectively.

The Agreement on cyber security, though intended to regulate the conduct of the United States and China alone, has had an effect on many prominent international cyber-related issues. As noted previously, there is deep ideological difference in how governments perceive cyber security. "Western countries have to come up with their own version of what these global norms should include. In the competition for intellectual leadership on global norms for cyber security, it is not enough to simply critique China's and Russia's offering" (Meyer 2015:58). It is inconceivable to resolve these ideological differences immediately, but in the interim, states can postulate international cyber security norms based on common interests. A United States Department of State strategy paper on international cooperation on cyber security suggests that:

> [c]oncrete measures probably will be most achievable initially on a bilateral basis . . . the Department of State should focus on cyber relationships with countries having concerns and interests congruent with ours. Bilateral [confidence-building measures] CBMs could then be extended to other countries to create broader coalitions (Hurwitz 2013:326).

International regime analysts would argue that in order to achieve a bilateral agreement with China on cyber norms, the United States had to focus on issues that had a high-level of depth: cyber issues that already had rules, that were compatible, and that were mutually reinforcing (Nye 2014:9). The Agreement relies on the principle that businesses' proprietary intellectual property rights information should be protected from cyber technologies and that states should cooperate with one another against cyber-enabled terrorism. Since the protection of intellectual property and terrorism deterrence are mutual concerns of the United States and China and are governed by an established normative framework in the international community, both countries were able to leverage their shared concerns to develop a standard of regulation. This led to a compromise between the two countries, and the bilateral negotiations provided a framework for other nation-states to coordinate their diplomatic conversations on cyber security.

Regime theorists would propose that standards that develop from bilateral agreements and cyber group initiatives within the regime complex of cyber allow for malleable cyber governance. This is uniquely important because technology is a phenomenon that is rapidly improving and changing and that requires norms and principles that can evolve with it. The strength and usefulness of bilateral agreements, the GGE contributions, the London and Budapest conferences, and the development of CERT contributions to cyber governance increases when influential states are involved.

The United States' dialogue with China focused on sub-issues within the cyber regime complex that mutually impacted both countries, a rationale known as complex independence. Focusing on the issue of freedom of information was not a realistic cyber sub-issue that could have garnered the support of China because China and the United States differ greatly on how the issue should be handled. Given this situation, the United States reflected the "rational self-interest of states seeking the benefits of cooperative solutions to collective action problems" (Nye 2014:11). The United States had to be very specific about the sub-issues it selected to negotiate with China in order to achieve Chinese support for sub-issues of concern to the United States.

Engaging the Needs of the Private Sector

The private sector, in particular large commercial business enterprises, is a major contributor to the United States' capitalist economic system and a critical stakeholder in cyber security. The private sector relies on the value of its intellectual property and secure communications. Small and large corporations, as well as commercial and academic research and development firms, utilize information systems and cyberspace to connect with consumers, suppliers, and partners. Computers and cyberspace provide commercial-based benefits to expedite proprietary services, establish market footprints, and grow client bases. Cyberspace serves as a platform for stakeholders to expand their customer base to consumers in other areas of the world, which furthers their potential growth. Most governments seeking economic growth appear to understand that a business's profitability benefits their countries' economic strength. Therefore, it is in the state's interest to intercede on behalf of the business sector to enact policies that safeguard the private sector from cyber attacks.

It is interesting to note Google's exit from the Chinese market in 2010: this revealed some of the serious economic and political problems that private sector organizations have experienced when operating cyber-based functions in China. The Chinese government engaged in concerted efforts to steal Google's source code and violated the human rights of Chinese activists by intruding into their Gmail accounts (Nye 2010:13). As a condition of doing business in China, Google was required to censor Internet searches on its China-based search engine, Google.cn. Although Google had complied with China's demands for four years, the company decided to discontinue the censorship service and removed itself from the Chinese market in 2010 (Nye 2010:13). The turning point for Google appears to have been when it recognized that performing these actions was becoming too costly for its business and tarnishing its image in the global community. Its economic survival required that Google maintain a competitive edge against United States companies like Microsoft. In addition, the company needed to preserve its reputation for being a secure Internet company. Google's departure had a domino effect: "Google's business partners experienced substantial business losses . . . various Chinese contracts had to change their strategies or exit the market at a high cost" (Tan 2012:476). The United States realized the significance of China's control on United States companies and understood that a fallout could seriously impact the United States economy.

"International Strategy for Cyberspace" seeks to promote economic development through "sustain[ing] a free-trade environment that encourages technological innovation on accessible, globally linked networks" (17). International regime theorists would argue that the United States decided to act as a utility maximizer in which "an actor striving for wealth . . . may cooperate in situations and will generally be inclined to accept constraints to achieve cooperation" (Gehring 1992:27). The United States negotiated with China, even if this meant losing the human rights battle, because the United States was concerned with protecting and advancing its economic wealth.

About the same time of Google's departure from China, United States Secretary of State Hillary Clinton expressed a United States interest in open dialogue and intergovernmental cooperation on Internet freedom during a speech at the Newseum in Washington, DC. Throughout her speech, she discussed several examples of politically-motivated censorship and mentioned the impact that failing to establish cyber norms had had on the business sector. She informed the audience that "a publicly listed company in Tunisia or Vietnam that operates in an environment of censorship will always trade at a discount relative to an identical firm in a free society" (Clinton 2010: Newseum Speech). She leveraged the Google departure to reiterate the need to develop an understanding and agreement with Chinese authorities. United States companies like Google, even though created in a "free society," are subjected to trade restrictions when they operate in states that practice censorship. These restrictions may impact companies' profit margins and creditability globally, which may also hurt the United States economy and political influence.

Human rights are also sub-issues of the cyber regime complex. They are not only political interests of the United States and other nations but also of ethical concern for many companies. In June 2012, the United Nations Human Rights Council "affirmed that the same rights that people have off-line must also be protected online." However, different countries have interpreted articles 19 (freedom of opinion and expression) and 29 (morality, public order, and general welfare) of the 1948 Universal Declaration of Human Rights differently (Nye 2014:11). Secretary of State Clinton did mention the issue of human rights in her speech, but there is a blatant difference of opinion on human rights issues between the United States and China. Regime theorists understand that "agreements are difficult to achieve in a world of independent, individualistic actors" and that states have to prioritize their interests and engage to find common ground (Bovcon 2011:9).

According to "International Strategy on Cyberspace," the United States' international policies on cyberspace factor in the need to protect the private sector, for the sake of the country's economic survival, meaning that the United States has thus made the protection of intellectual property a major focus in the Agreement. China has a history of intruding in or stealing information from American information systems. In 2009, for example, Operation Aurora was able to trace malware that affected thirty United States companies, including Google and Northrop Grumman, back to a Beijing company connected to China's People's Liberation Army (PLA) (Knowledge@Wharton 2014).

> The PLA [China's military] is responsible for most hacking against the United States. Some of this is the normal political-military espionage that the United States itself is well-known [for]. But local PLA units also hack to make money. It is a source of private income when they steal commercial secrets and sell them to Chinese companies for cash or favors (Lewis 2015).

Given the international law of state responsibility, the United States could conceivably use the cyber regime complex to hold China responsible for illicit cyber acts against the United States (Moore 2013:243).

Stealing intellectual property from the United States gives China an unfair economic advantage and impacts the economic growth of the United States and its national security. "International Strategy for Cyberspace" explains the consequences of intellectual property theft and the United States' response as follows: "Results can range from unfair competition to the bankrupting of entire firms . . . The United States will take measures to identify and respond to such actions to help build an international environment that recognizes such acts as unlawful and impermissible, and hold such actors accountable" (17).

The Agreement was designed to advance the United States' policy on international cyberspace. According to the White House, both countries agreed that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors" (White House Press Release 2014). The United States and China have agreed that the theft of intellectual property is impermissible. The Agreement allows the United States to hold China responsible for intellectual theft originating out of the East Asian country, regardless of whether or not the attacker is an independent actor acting under the instructions of the Chinese government.

International regime theory would justify the Agreement as an advancement of the regime complex. Regime analysts would argue that "shared expectations about appropriate behavior and by upgrading the level of transparency in the issue area . . . help states (and other actors) to cooperate . . . and reap gains on welfare or security" (Karns and Mingst 2010:43). Cooperating on shared expectations is a generally accepted concept for regimes. This could be applied to the cyber regime complex. In this instance, security is connected to economic stability. The United States and China are economically tied closely together, and both nations have benefited from the relationship.

Conclusion

This paper has addressed the question why the United States adopted a bilateral agreement on cyber security with China in September 2015. Cyber attacks originating in China actively threatened the United States' information systems for several years leading up to the Agreement, and they continue to do so. The OPM hack in early-2015 was allegedly orchestrated by the Chinese. In addition, the theft of intellectual property by PLA members over a span of eight years led to an indictment by DOJ in 2014. These hacks have exposed American vulnerabilities and threaten the country's overall security. Through the lens of international regime theory, this paper has argued that the United States entered into formal negotiations with China in September 2015 to: 1) clarify the application of cyber norms in the international system; 2) identify core security issues affecting states in order to sponsor collaboration between "like-minded" and "other-minded" states; and 3) establish behavioral limits on the private sector to protect the economic and national security concerns of the United States.

Under the rubric of regime theory, state actors seek to advance their own interests through international regimes. Currently, cyber does not have its own regime, but it does borrow norms, principles, and decision making procedures from other regimes, institutions, and practices to develop its own regime complex. The United States has utilized other regimes and created the Agreement for it to be applied to the cyber regime complex. Since customary international law lacks sufficiently-clear norms to regulate a cyber regime as such, the United States and China decided to clarify certain subset issues of cyber. The United States' ability to identify topics relevant to cyber security in the Agreement contributed to the regulation of cyber activities through the cyber regime complex.

The Agreement advanced the United States' own security concerns by focusing "like-minded" issues with "other-minded" states. According to regime theory, the application of complex interdependence required the United States to compromise in order to achieve cooperation with China. Although it was not able to agree with China on some issues, the United

States was able to reach an agreement on other matters that affected both countries. Lastly, the United States included intellectual property theft in the Agreement to address a wider concern of loosely related issues of cyber security: human rights and economic development. A significant concern for the United States was the economic impact cyber intellectual property theft would have on the country if left unregulated. Developing a working bilateral relationship with China on cyber activities was a method for the United States to protect and advance its own interests.

References

Bovcon, Maja. 2013. Françafrique and Regime Theory. *European Journal of International Relations* 19(1): 5-26.

Clinton, Hilary Rodham. Remarks on Internet Freedom. Speech at The Newseum, Washington, DC, Jan. 21, 2010.

Dunne, Tim and Marianne Hanson. 2013. Human Rights in International Relations. *Human Rights: Politics and Practice*. <http://socialsciences.exeter.ac.uk/politics/research/readingroom/Dunne-goodhart-chap04.pdf>. (Accessed Apr. 23, 2016).

Gehring, Thomas. 1994. *Dynamic International Regimes: Institutions for International Environmental Governance*. Los Angeles: Peter Lang.

Griffiths, Martin, M. Scott Solomon, and Steven C. Roach. 2009. *Fifty Key Thinkers in International Relations*. London: Routledge.

Haggard, Stephan and Beth A. Simmons. 1987. Theories of International Regimes*. International Organization* 41(3): 491-517.

Hurwitz, Roger. 2014. The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests* 36(5): 322-31.

Ilie, Marian, Antonio-Silviu Mutulescu, Diana Anca Artene, Sofia Bratu, and Florin Făinişi. 2011. International Cyber Security Through Co-Operation. *Economics, Management, and Financial Markets* 6(2): 438-48.

Inkster, N. 2013. Conflict Foretold: America and China. *Survival* 55(5): 7-28.

Karns, Margaret and Karen Mingst. 2010. *International Organizations: The Politics and Processes of Global Governance* 2d. Boulder: Lynne Rienner.

Keohane, Robert and Joseph Nye. 2011. *Power and Interdependence* 4d. New York: Pearson.

Lewis, James Andrew. 2015. "Moving Forward with the Obama-Xi Cybersecurity Agreement." *Center for Strategic and International Studies*. <https://www.csis.org/analysis/moving-forward-obama-xi-cybersecurity-agreement> (Accessed April 20, 2016).

Lifland, Amy. 2012. Cyberwar. *Harvard International Review* 33(4): 7-8.

Lindsay, Jon R. 2014. The Impact of China on Cybersecurity. *International Security* 39(3): 7-47.

Majeski, Stephen. Lecture Notes. "After Hegemony." University of Washington, Seattle. <http://faculty.washington.edu/majeski/426.04/lecture7.html> (Accessed May 3, 2016).

Meyer, Paul. 2015. Seizing the Diplomatic Initiative to Control Cyber Conflict. *The Washington Quarterly* 38(2): 47-61.

Moore, Stephen. 2013. Cyber Attacks and the Beginnings of an International Cyber Treaty. *North Carolina Journal of International Law and Commercial Regulation* 39(1): 223-57.

Nakashima, Ellen. 2015. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say." *Washington Post*, July 9, 2015. <https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/> (Accessed Mar. 30, 2016).

National Committee on American Foreign Policy. *Cyberpower and National Security*. 2013. *American Foreign Policy Interests* 35(1): 45-58.

Nguyen, Reese. 2013. Navigating *Jus Ad Bellum* in the Age of Cyber Warfare. *California Law Review* 101(4): 1079-1129.

Nye, Joseph. 2010. Cyber Power. *The Future of Power in the 21st Century*. Cambridge: Harvard. <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf> (Accessed May 3, 2016).

Nye, Joseph. 2014. *The Regime Complex for Managing Global Cyber Activities*. London: Chatham House.

Sarkesian, Sam C., John A. Williams, and Stephen J. Cimbala. 2013. *US National Security: Policymakers, Processes, and Politics* 5th. Boulder: Lynne Rienner.

Schmitt, Michael. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press.

Spalević, Žaklina. 2014. Cyber Security as a Global Challenge Today. *Sinteza* 687-92.

Tan, Justin and Anna Tan. 2012. Business Under Threat, Technology Under Attack, Ethics Under Fire: The Experience of Google in China. *Journal of Business Ethics* 110(4): 469-79.

"The Download on the U.S.-China Cyber Espionage Agreement." Knowledge@Wharton, Sept. 30, 2015. <http://knowledge.wharton.upenn.edu/article/the-download-on-the-u-s-china-cyber-espionage-agreement/> (Accessed May 2, 2016).

United States Department of Justice Office of Public Affairs. 2014. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> (Accessed Apr. 5, 2016).

United States Office of the President. 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," Washington, DC.

<https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> (Accessed Apr. 28, 2016).

Vaishnav, Chintan, Nazli Choucri, and David Clark. 2013. Cyber International Relations as an Integrated System. *Environment Systems and Decisions* 33(4): 561-76.

White House Office of the Press Secretary. 2015. "Fact Sheet: President Xi Jinping's State Visit To The United States." <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (Accessed Apr. 5, 2016).