國際學碩士學位論文

Cyber Security and International Cooperation:

An Analysis on U.S.-China Stance Difference

Cyber Security와 국제협력:

중국과 미국의 입장차이 분석을 중심으로

2013年 2月

서울大學校 國際大學院

國際學科 國際協力 專攻

林寶英

Cyber Security and International Cooperation:

An Analysis on U.S.-China Stance Difference

Thesis by

Boyoung Lim

Graduate Program in International Cooperation

For the degree of Masters of International Studies

February 2013

Graduate School of International Studies
Seoul National University

Seoul, Korea

Cyber Security and International Cooperation:

An Analysis on U.S.-China Stance Difference

Cyber Security와 국제협력:

중국과 미국의 입장차이 분석을 중심으로

指導敎授 辛星昊

이 論文을 國際學碩士學位論文으로 提出함

2013年 2月

서울大學校 國際大學院

國際學科 國際協力專攻

林寶英

林寶英의 國際學碩士學位論文을 認准함

2013年 2月

委 員 長 趙 英 男 (印)

副 委 員 長 金 泰 均 (印)

指 導 敎 授 辛 星 昊 (印)

THESIS ACCEPTANCE CERTIFICATE

The undersigned, appointed by

The Graduate School of International Studies

Seoul National University

Have examined the thesis entitled

Cyber Security and International Cooperation:

An Analysis on U.S.-China Stance Difference

Presented by **Boyoung Lim,**

Candidate for the degree of Masters of International Studies, and hereby certify that the examined thesis is worthy of acceptance:

Signature _____
Committee Chair **Cho, Young-Nam**

Signature _____
Committee Vice Chair **Kim, Taekyoon**

Signature _____
Committee Member **Sheen, Seong-Ho**

Date: February 2013

ABSTRACT (ENGLISH)

Cyber Security and International Cooperation:
An Analysis on U.S.-China Stance Difference

This work aims to analyze the stances of U.S. and China on cyber security, which is nowadays one of the most important international issues, thereby discussing the possibility and form of international cooperation in global governance of the cyberspace and against cyber threats. To illustrate the importance and uniqueness of this issue, this paper discusses the attributes of the cyberspace and what cybersecurity means. The global nature of the cyberspace has blurred the traditional distinction between the concept of war and crime, thus has made international cooperation indispensable in dealing with cybersecurity issues. In addition, states relied on "hard (codified)" international law in order to enable long-standing international cooperation in traditional security issues, such as arms control agreements. Also, unlike traditional security issues, in which states were the main actors, cybersecurity involves a wide variety of actors including non-state actors. Although states and international actors should commit to cooperation with non-state actors as well, current discourse on cybersecurity reveals that most states perceive cybersecurity as a critical area of national security, so states are still the major actors in the international cooperation of cybersecurity. The United States and China are the two major influential players in international affairs, and both have very different views on what cybersecurity is and how it should be achieved. This stance difference, along with

the discourse in the United Nations General Assembly First Committee which points towards international legal issues such as national sovereignty as the next focal issue in the third Group of Governmental experts, are examined under the analytical framework based on Abbot & Snidal (2000)'s work on hard and soft international law. This paper concludes that international cooperation on cybersecurity is more likely to depend on soft international law, thereby increasing the role of soft international law in international governance.

TABLE OF CONTENTS

I. INTRODUCTION

1. Research Question

The world today has never been more connected in human history. Owing to the remarkable progress people made in information technology, which was marked by the advent of the Internet, it became possible to overcome the barriers of time and space in the cyberspace. Now it takes only a few seconds for people to communicate with each other from halfway around the world, and regional events can have global implications. But this works in the same way for threats to security, which is the case of cybersecurity issues actively discussed on the international level. President Barack Obama's 2011 Cyberspace Policy Review declared that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century," and many state and non-state actors have recognized that without cooperation no one can single-handedly resolve problems in the field.

Will the difference in opinion and interest among states and governments preclude international cooperation for cybersecurity of any kind? If traditional ways of ensuring long-term international cooperation, such as formal treaties ("hard" international law), are not feasible in the case of cybersecurity, as some have argued, what kind of cooperation will be possible? Can soft law play a bigger role in international governance of cybersecurity issues? This paper aims to identify the stance difference between the United States and China in their perspectives of cybersecurity to answer these questions.

International law is one of the most effective ways to ensure long-standing international cooperation and state commitment. At the same it is basically the product of extended negotiations among states, and "each state has its own stake in controlling certain behaviors, and these behaviors differ." Thus, the stances of states which wield considerable amount of influence in international relations at the initial stage of the formation of international law in a certain issue area heavily influences the form of international interactions within that issue area.

Among all states, it is evident that the United States and China are the two most influential states in the international arena in all aspects. Liberthal & Singer (2012) have noticed the "spillover effect" of cybersecurity on the bilateral relationship between the U.S. and China, and Goldsmith & Wu (2006) have especially noted that "China is an enormous force that is changing the Internet's identity," in that the Internet in China is quite different from what the Internet was like when it was first 'invented' in the United States. Recently, these two states, the United States and China, have agreed to cooperate on cybersecurity. Chinese Defense Minister Gen. Liang Guanglie and U.S. Defense Secretary Leon Panetta announced in a joint statement that it is "critical" for China and the U.S. to work together on cybersecurity issues in order to avoid any "miscalculation or misperception" that could provoke a crisis. This shows that the two great powers have started to recognize the significance of the issue they face, but at the same time what the announcement implies is that there certainly *exists* a possibility of such miscalculations or misperceptions. Then, *why* and from *where* does this possibility arise? *What* supports this belief?

a. Research Goals

By examining the stance difference on cybersecurity between the United States and China, this paper aims to specify the red lines between the perspectives of the two to draw the implications for the possibility of international cooperation in cybersecurity. Compared to other issues of both international and national security, cybersecurity is an ambiguous and amorphous concept. There is no universal definition of 'cybersecurity'; there is an ongoing debate on the impact cyberspace and networked technology has on warfare and international relations in general.

To date, some states, including the United States, have tried to defend their national interests that are connected or related to the cyberspace by unitary action. However, the NRC Committee of the United States has recently noted that "measures associated with classical deterrence are difficult to employ against cyberattacks and exploitation," and accordingly the Executive branch and Congress are looking for "ways in which international cooperation and agreements could enhance cybersecurity." Although it is still not clear what the definition of cybersecurity is, the central role and importance of international cooperation and agreements in cybersecurity issues seems to be evident.

b. Research Significance

Understanding the stance difference between the U.S. and China has significance in that it can contribute to the perspectives of both international politics and international law in understanding cybersecurity. Long-standing international cooperation is made

possible by political agreements in the form of international law, which is a result of extended negotiation among states. Since cybersecurity is a relatively new issue, states have and will continue to utilize their resources to influence this negotiation process. From the international politics perspective, knowing to what extent the U.S. and China differ in their views on cybersecurity will help understand the dynamics of cyber norm emergence and the following developments of international regimes and institutions.

From the international law point of view, as will be discussed in detail below, international legal issues regarding sovereignty and state responsibility will become the central issues of cybersecurity discussions. In this context, knowing the different perceptions of negotiating parties may not only prevent misunderstandings, but may help participants seek mutual concessions and ways to reach agreements.

At the same time the two states represent very different, if not opposite, views on the proper use and future of the Internet. In their 2012 report, Liberthal and Singer have stressed the need for bilateral dialogues between the U.S. and China on cybersecurity, because "the spillover effects of cybersecurity on the broader U.S.-China relationship is also perhaps more critical than for any other bilateral relationship." While the authors have rightly recognized the significance of U.S.-China bilateral relationship in the cybersecurity realm, and also have mentioned there exists a huge gap between how the two states view cybersecurity, the primary purpose of their research was to "suggest how to take the particular characteristics of the cyber security realm into account while fostering U.S-China cooperation on cybersecurity." The report itself is more of a general overview for those who are not familiar with technical concepts and the cyberspace, and

touches upon neither the specific issues of dispute nor consent. Given the weight U.S. and China possesses in this issue, proper understanding of the position each hold in protecting the cyberspace may be used as a guidance in understanding how other states, and states in general, view the issue of cybersecurity, with U.S. and China both standing at the very edge of the spectrum.

Another reason for conducting an analysis on stance difference between U.S. and China is to provide a basis for future research on stance differences among states on cybersecurity issues. Apart from the works of ITU (2005), Maurer (2011), Liberthal & Singer (2012), there is a lack of prior research directly dealing with the position of states on issues involving cybersecurity. Even each of the existing works in this field have different focus points. Liberthal & Singer concentrates on ways to consider the unique characteristics of cybersecurity in promoting cooperation between U.S. and China, and Maurer tends to seek evidences supporting norm emergence in the United Nations regarding cybersecurity. Meanwhile, the 2005 report from ITU has introduced the cybersecurity initiatives of many states and pointed out certain problems and prospects for an international regime for the protection of cyberspace, but has neglected China in its scope of analysis, and seems to be more interested in identifying common themes and best practices in order to show possible problems in forging a 'global culture of cybersecurity', rather than revealing potential issues of disputes between certain countries.

Currently there are many international forums in which cybersecurity issues are discussed. Even in the United Nations the activities regarding this issue is fragmented. Although states have not reached an agreement on which forum is legitimate to hold

discussions of cybersecurity, the United Nations General Assembly First Committee, which deals with disarmament and international security, has made remarkable developments in that they made multilateral efforts to share the views of each state on this issue by organizing the Group of Governmental Experts, which produced a successful report in 2010. By requesting states to give official statements on how they perceive cybersecurity issues to the Secretary General.

In addition, the governments of the U.S. and China have both announced their official perspectives on cybersecurity, in 2011 and 2010, respectively. These government documents reveal which values they prioritize the most in considering cybersecurity and the reasons for their claims. Therefore, this paper will focus on the statements made by the U.S. and China in the UNGA First Committee and additionally draw from the government documents to identify how their perspectives evolved over time and how their opinions differ.

2. Methodology

a. Comparative Analysis by Archeological Approach

With the abundance of information available from UN official documents, it is both necessary and possible to get a more "comprehensive picture on how countries across the globe think about the issue and how their thinking evolved over time." Therefore, this paper will conduct a comparative analysis on the stances of the United States and China by taking the 'archeological' approach to international institutions introduced by Keohane,

which seeks to examine the "differences in the ideas and ideologies held by dominant groups (...) at the time when various multilateral arrangements were instituted." Although there is yet to exist a full-fledged international institution regarding the governance of cybersecurity issues due to its relative recentness, states (especially both the United States and China), regardless of the type of issue at stake, have been active in international forums and discussion tables in order to reflect their own opinions and shape international discourse in a way that is favorable to its own national interests.

b. Analytical Framework

Some have argued that codified international treaties, such as the Convention on Cybercrime, no longer can play a significant role in ensuring state compliance, due to the attributes of cybersecurity. They even go as far as to claim that the future of the Internet will reflect "the interests of powerful nations and the conflicts within and between them." From hindsight, current events partly support their forecast, but partly not, in the case of the World Conference on International Telecommunications, in which the International telecommunication Regulations has been revised in a way that allows a higher possibility of government control over the Internet. The revision was agreed by a majority of states that are not necessarily 'powerful' in international politics, while states that disagreed on the revision were mostly the wealthy western states.

Focusing on how states actually perceive values and cyber-threats, the perception gap among states as to which values should be secured from what threats may cause each state to reach different solutions, mainly because 'states vary widely in the value they

place on security.' This difference, in turn, reflects each state's perceptions on national security and political concerns and consequently acts as a barrier toward international agreements. As mentioned above, the disagreement on 'hate speech' among states has been one of the main factors that caused the delay in reaching an agreement in the negotiating process of the Convention on Cybercrime. Goldsmith & Wu (2006) have pointed out the limits of "hard" cooperation based on codified (hard) international law in regulating cybercrime and eliminating cyber-attacks. Negotiations on such issues will be difficult to result in agreements as states are reluctant to limit their state sovereignty, and even if they do reach an agreement, under the circumstances of cybersecurity it is unlikely that all non-state actors will agree to comply.

If cooperation based on "hard" law is infeasible in promoting cybersecurity, "soft" law could be a potential alternative. In fact, some scholars have shed light on the role soft law can play in international governance. Abbott and Snidal (2000) have argued that although some neglect or underestimate soft law, it can sometimes be preferred over hard law. In their work, hard and soft law are not dichotomized concepts; rather, they explain it as a gradation of a continuum evaluated on the basis of three criteria, which are obligation, precision, and delegation. Thus, hard law requires a high level of obligation, precision and delegation, while soft law is "softer" in the sense that it requires a low level of some or all of the criteria. Although hard law has many advantages such as "reduc[ing] the cost of operating within a legal framework," they are hard to reach, whereas soft law can "lower the cost of achieving (some) legalization in the first place."

Especially when international arrangements impinge on *state sovereignty*, states are

reluctant to join the discussions that might possibly limit their powers. Thus "states face tradeoffs between the benefits and sovereignty costs of different forms of legalization," and "sovereignty costs are especially high in areas related to national security." As cybersecurity is viewed by many states as an indispensable part of national security, and because the attribution procedure requires the core functions of state sovereignty, in the case of cybersecurity "states can limit sovereignty costs through arrangements that are non-binding or imprecise or do not delegate extensive powers."

Also, being a relatively *new and complex* international issue, the lack of agreed-upon definitions of concepts related to cybersecurity may increase uncertainty of making a binding agreement to the extent that "precision [is] less desirable as well as attainable." In this case soft law can provide a framework in which "states can work to resolve their uncertainty, making harder legalization more attractive."

Probably the most interesting case in which soft law is preferred over hard law relevant to this paper would be when the "*degree of divergence* among the preferences and capacities of states" is high, and the issue requires the cooperation from a majority of states. As discussed earlier, although many researchers have recognized that states show huge differences in the way they view cybersecurity issues, there has not been prior research focusing on the stance difference between two specific states. "When principles intersect, one who must resolve the conflict must attempt to take into account both sides, so that both colliding principles are satisfied to the maximum extent possible." However, there still remains a question as to how much the United States and China differ in their views of cybersecurity.

In sum, the analysis of the stance difference of U.S. and China on cybersecurity will be based upon three main criteria (high sovereignty costs, uncertainty due to recentness, and degree of divergence among state preferences and capacities) pointed out in Abbott & Snidal's work on the role soft law can play in international governance.

c. Data Sources and Materials

In order to analyze the stance difference between U.S. and China in terms of how they view cybersecurity, this work will first examine the UN First Committee documents and the official documents produced by both governments, and then turn to domestic discussions in both countries.

1) Primary Source

Since 1999, 49 states, including the U.S.(3 times: 1999, 2004, 2011) and China (4 times: 2004, 2006, 2007, 2008), have offered their official views on various aspects of cybersecurity, and these statements are available in the form of <The Report of the Secretary General> from the UN Official Document System. Because both the United States and China has shown their stances several times, these materials provide information on how their perspectives have evolved over time: what has changed and what has remained the same. This can help identify the red line between the two states. Seven documents (A/54/213, A/59/116, A/59/116/Add.1, A/61/161, A/62/98, A/63,139,

A/66/152) will be analyzed to examine the perspectives both states offered in the UN First Committee, which is responsible of "dealing with disarmament, global challenges, and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime."

To examine the details of their perspectives on cybersecurity, the government official documents of both shall be analyzed. Recently, both governments have announced official documents representing the official perspectives on cybersecurity. In 2010, the State Council Information Office of the People's Republic of China (中国人民共和国国务院新闻办公室) announced the first white paper ('The Internet in China'/ 中国互联网状况) in which they outlined the current situation of the Internet in China and the principles the Chinese government maintain on Internet usage and regulation over the cyberspace. In 2011, the White House also released an official document ('International Strategy for Cyberspace') that mostly focused on the principles the United States claims to be the fundamental basis for cybersecurity.

2) Secondary Source

In addition to the analysis of primary source materials, it is important to examine the discourse formed in both states regarding cybersecurity, since in many cases the opinions of scholars and experts are reflected in government policies and works as a reference in the decision-making process. This work has focused on the domestic literature of both

states relevant to the following three topics:

(1) How scholars in each state evaluate their own national cybersecurity strategy / How they approach cybersecurity in general;

(2) How scholars in each state perceive the other (in China's case, the United States; in the United State's case, China) in the context of cybersecurity; and

(3) How scholars in each state view international relations in cybersecurity.

The following table lists the works that are analyzed in this work.

United States	Topics	China
1) <State-level Cybersecurity> 2) <White House and Department of Defense Announce Strategies to Promote Cybersecurity, including strengthening norms affecting internet security> 3) <The need for a national cybersecurity research and development agenda>	How scholars in each state evaluate their own national cybersecurity strategy / How they approach cybersecurity in general	1)《我国国家网络空间安全战略的理论构建与实现路径》 2)《依法保障信息网络安全》 3)《中国国家信息安全与策略研究》
1) <Cybersecurity and U.S.-China Relations> 2) <Cyberwar : The United States and China Prepare for the Next Generation of Conflict> 3) <Defending America Against Chinese Cyber Espionage Through the Use of Active Defense>	How scholars in each state perceive the other in the context of cybersecurity	1)《中美在网络空间的分歧与合作路径》 2)《网络空间中的中美关系》 3)《美国《网络空间国际战略》评析》 4)《美国输出价值观的新 "武器"》
1) <Cyberwar: The Future of Conflict> 2) <Cyber Warfare: A "Nuclear Option"?>	How scholars in each state view international relations in cybersecurity, and cyber warfare	1)《浅析信息时代国际网络安全形势与我国对策》 2)《网络安全离不开国际关系》 3)《互联网的国际博弈与合作研究》

3. Literature Review

Although international cooperation in the cybersecurity realm is a pressing issue, attention towards this topic has been increasing very recently. This section will start by reviewing works on topics relevant to cybersecurity focusing on those related to international relations. Then it will take a brief look at how the two states

a. Cybersecurity Discourse and International Relations

Maurer (2011) has compiled the various activities and discussions that have been taking place in the UN since 1999, when Russia first proposed a draft resolution that initiated the agenda titled "Developments in the field of information and telecommunications in the context of international security." He has argued that there is strong evidence that supports norm emergence in the UN cybersecurity discourse, and states are actively taking part in this process as norm entrepreneurs.

Following the works in the UN General Assembly First Committee (which deals with disarmament, global challenges and threats to peace that affect the international community) since 1999, 49 states have sent statements the the UN Secretary General regarding their positions and views on cybersecurity. A close examination on these statements show the official positions on cybersecurity each state holds. The UN Secretary General has made the following remarks for the report produced by the second GGE(Group of Governmental Experts):

> "The General Assembly has an important role to play in the process of making information technology and telecommunications more secure, both nationally and internationally. Dialogue among Member States will be essential for developing common perspectives. Practical cooperation is also vital, to share best practices, exchange information and build capacity in developing countries, and to reduce the risk of misperception, which could hinder the international community's ability to manage major incidents in cyberspace. (...) The present report is meant to serve as an initial step toward building the international framework for security and stability that these new technologies require."

Eneken Tikk-Ringas has identified the main issues and outlined the process that has took place in the first committee between 1999 and 2012 in a Cyber Policy Process Brief for ICT4peace. According to her analysis on the statements made by states to the UN Secretary General, she observed a consensus on the general need for international cooperation and collaboration for the purpose of global information security which is the result of the second GGE, but still there exists a deep perception gap between states as to the definition and scope of it. What is most noticeable is the stance difference between the two blocs, which she describes as "the US and other liberal democracies on the one side and the Shanghai Cooperation Organization (SCO) countries on the other," in issues of "key definitions; exact scoping of the topic; threat perception as well as the mandate and role of the UN in general and the First Committee in particular in resolving international information security issues. The western bloc, which is represented by the US, has emphasized on the free flow of information, and has shown a willingness to limit

the role of the First Committee in cybersecurity, while member states of the SCO have argued that each government has the right to manage its own cyberspace in accordance with its domestic legislation, as China has stated, and have projected the UN and the First Committee as "an appropriate forum to address a wide spectrum of threats to include military, terrorist, and criminal uses of ICT." In line with Maurer's argument, she has also observed proposals for developing politically binding norms of acceptable state behavior in cyberspace. Based on the developments in the First Committee, she concludes that:

> "It is expected that the *legal issues* (such as the applicability of the law governing the use of force, the law of armed conflict, implementation and interpreting of the legal concepts of sovereignty and state responsibility) *will form a considerable part of the third round of GGE discussions*. Another open issue,(...) is the division of information security tasks between national government and the international community. Several countries have pointed out the protection of information and information-based systems as a responsibility for governments, while others have emphasized the need for international cooperation and collective measures. Further, the *disagreement between the US-led wing and the SCO countries* on the Internet governance model is likely to shape discussions."

In sum, using the words of Chadwick, "powerful nation-states may try to ensure that their legal norms are simply writ large at the international level." As Maurer and Tikk-Ringas have pointed out respectively, the discussion on cybersecurity in the UN is growing, and the discussion in the First Committee is expected to focus on those related

to international legal issues.

b. Cybersecurity and States: Crime or War?

If the cybersecurity discourse in the UN is anticipated to center on international legal issues related to state sovereignty, responsibility, and those related to armed conflict in cyberspace in the near future, it is important to know how states now think of sovereignty and "cyber-warfare." Therefore, this section will introduce some prior research providing insight to how states came to perceive the influence of cyber threats upon their state sovereignty and security in general, and then look into the domestic literature of both states related to this topic.

As early as 1997, Timothy S. Wu provided a basis for discussions on the Internet regulation and the international system. The interesting part of his research is the application of the liberal theory to think of the Internet less as a place and more as a regime of transnational norms and rules. Wu made a sharp analysis in pointing out two important constraints in reaching a consensus on "cyberspace sovereignty" under the assumptions of the liberal theory. First, it is improbable that most people will oppose state regulation on actions in cyberspace that have negative effects on real space, such as cybercrime. Second, the norms of a free cyberspace, or "cyberspace sovereignty", will be more readily accepted by individuals in the United States and like-minded countries; on the other hand, appeals to free speech protection of the type guaranteed under the First Amendment "will fall on deaf ears in many countries". Additionally, he also indicates another set of limitations regarding the transmission of consensus to the level of state

preference. Governing structure of states may differ, so depending on specific governing structure of each state, the interests of those who support the idea of a free Internet may not be adopted as state policy.

Wu's observation leads us to the following conclusion: it may be relatively easier for states find a way to cooperate with each other in *combatting cybercrime*, while it may be much more difficult to reach a consensus on norms involving *how to regulate the cyberspace*, or *to what extent states should interfere in cyberspace*.

Nearly a decade later, again in 2006 Wu published a book with Jack Goldsmith in which he argued that the most fundamental roles of governments will not be diminished by the growing role of Internet, despite some changes the Internet may bring to the ways territorial states govern. Rather than accepting the majority assessment of globalization which views the Internet as the "essential catalyst of contemporary globalization" which would eventually contribute in diminishing the relevance of borders, territory, and location, thereby undermining the territorial nation-states' role as the central institution for governing human affairs, they provide a series of evidences to support their main argument, which is that the destiny of the Internet over the next decades will *reflect the interests of powerful nations and the conflicts within and between them*:

> It is that the United States, China, and Europe are using their coercive powers to establish different visions of what the Internet might be. In so doing, they will attract other nations to choose among models of control ranging from the ***United States's relatively free and open model*** to ***China's model of political control***. The

> result is the beginning of a ***technological version of the cold war***, with each side pushing its own vision of the Internet's future [Italics and emphasis made by the author].

Goldsmith and Wu's acute observation that in the following decades the *interests of powerful states and the conflicts between them* will be reflected in the discussion of Internet control seems to be partly supported by a book written by Richard A. Clarke and Robert K. Knake. The authors claim that the United States, until 2009, had almost "single-handedly" blocked arms control in cyberspace, as the U.S. viewed the Russian proposal for a cyber arms control as largely a propaganda tool, and the U.S. had not yet explored what it wanted to do in the area of cyber war. Yet, Clarke claims that now the U.S. has "gained a better understanding of what cyber war could look like, it may be time for the United States to review its position on cyber arms control".

On that point, Maurer's work on cyber norm emergence at the United Nations provides a better way to analyze the disagreements among states on issues involving cybersecurity. As mentioned above, while the purpose of Maurer's research centers on showing the dynamic process of cyber norm emergence, the process of cyber norm emergence itself reflects the *interests of powerful nations and the conflicts within and between them*, mainly between the U.S., Russia and China. States play an important role as norm entrepreneurs in the UN cybersecurity discourse. Maurer divides the norm emergence process at the United Nations into two main streams of negotiations: a **politico-military stream** which focuses on **cyber-warfare**, and an **economic stream**

focusing on **cybercrime**. Recalling Wu's 1997 paper which implied that it would be relatively easier for states to find common grounds in combatting cybercrime than reaching a consensus on norms involving how to regulate the cyberspace in general, Maurer's distinction, and of course, the activities related to cybersecurity in the United Nations, seems to be in line with Wu's early observation in that it distinguishes cyber-warfare from cybercrime.

What can be observed from prior research is the stunningly different, if not completely the opposite, stances the United States and China takes on these two issues, which is the starting point of this paper. Taking a closer look at the number of General Assembly resolutions adopted over time and the list of co-sponsors of draft resolutions listed in Maurer's work, one can identify a clear difference of position between U.S. and China. The U.S. had rejected Russia's proposal for a cyber arms control treaty in the politico-military stream up until 2010 when it finally reversed its objection to co-sponsor the Russian draft resolution in the First Committee. Quite the contrary, U.S. has persistently tried to step up international cooperation among law enforcement agencies in the United Nations. On the other hand, China has generally sided with Russia in the politico-military stream in calling for a cyber arms control treaty by joining as a co-sponsor for the first draft resolution proposed by Russia in both 1998, and also recently in 2011 issued a joint letter with the governments of Russia, Tajikistan and Uzbekistan, which included a draft "International code of conduct for information security". However, in the economic stream, China has not co-sponsored or supported any other draft resolution except for one resolution adopted by the General Assembly in 2005 on the

"Creation of a global culture of cybersecurity and the protection of critical information infrastructure", which includes a preambular paragraph stating "that each country will determine its own critical information infrastructure". Unlike its position in the politico-military stream, in the economic stream regarding issues of cybercrime China's position differed from that of Russia's depending on the situation. One such case is the resolution adopted without a vote by the General Assembly in 2002, which was introduced by the United States and 73 other member states including Russia and the Republic of Korea, but which China did not co-sponsor.

The following table simplifies the U.S. and China's positions on the two streams of negotiations taking place in the United Nations shown in Maurer (2011):

	U.S.	**China**
Politico-Military Stream (Cyber-Warfare/Arms Control)	No (Until 2010)	Yes
Economic Stream (Cybercrime)	Yes	No

<Table 1: Stances of U.S., China in UN Cybersecurity discourse>

The positions the two states take in each stream indeed supports the statement that "the U.S. and China represent very different views on the proper use and future of the Internet" which was made by Liberthal and Singer but was not properly addressed in their work. This reminds us of Goldstein and Wu's statement on future Internet control models, i.e., '***U.S.'s relatively free and open model*** vs. ***China's model of political control***,' as well as Wu's observation that '*states are more likely to reach an agreement in*

cybercrime issues than in agreeing upon to what extent states should be able to interfere in cyberspace'.

Then how does the U.S. and China actually view sovereignty issues in the cybersecurity context? As the academic discourse on cybersecurity in both states shall be reviewed in detail in Chapter 3, this section will briefly look into some domestic works on the relationship between state sovereignty and cybersecurity.

Chinese literature exert a bigger interest in this issue, and there are several works dedicated to this subject specifically. Most of these works calls for the concept of "Network/Internet sovereignty" and supports the right of the state to control and regulate the Internet within its territories. There is a tendency to perceive the cyberspace as strategically important, and propose measures through which China can safeguard its state sovereignty and national security.

One of the most recent and representative among these works is Cao Peng (曹鹏)'s work. According to Cao, the concept of "Network sovereignty (网络主权)" must be elicited by extending the concept of state sovereignty, since the cyberspace has become the fourth realm in which state has to protect its people, after territory, sea, water, and space. This is because the cyberspace has now become a strategic place in which states compete against each other, and this competition is directly related not only to a country's future influence in international relations, but also to its existence and development. Network security is defined as the states' right to control the cyberspace within its jurisdiction by regulating information, ensuring national security in the cyberspace, and

maintaining the right to independently participate in international activities related to information. However, the advent of the Internet has strengthened the sovereignty of developed countries, while at the same time it weakened those of the developing countries, which has furthered the inequality between developed and developing countries. The gap between developed and developing countries have been evident in technological development, which has been widened by the latter's dependence upon the former's monopoly in hardware and software technology, combined with the gap between the two in terms of discourse power in the international arena, have greatly contributed to the weakening of sovereignty of developing states, while boosting that of developed states. Cao suggests China to strengthen each and every aspect of its state sovereignty, that is, political sovereignty, economic sovereignty, and cultural sovereignty, against the threats to state sovereignty caused by the Internet, while taking a lead in making a new international order for governing cyberspace.

The United States also emphasizes the importance of sovereignty in cyberspace, but from a quite different aspect. Whereas most Chinese writers have focused on justifying the elicitation of network sovereignty, there is no prior research that directly concerns the strengthening or weakening of state sovereignty by cyberspace. In fact, those of the U.S. are more interested in the principles and norms related to cybersecurity. Some, including the government itself, have pointed out that existing customary and conventional legal norms are also applicable to the cyberspace, and therefore there is no need for a new international legal framework for conflicts in cyberspace. Rather, the right of a state to defend itself in armed attack against itself justifies its right to retain all necessary means,

including military, and use it against hostile acts in cyberspace. At the same time, it claims that this is far from "militarizing" the cyberspace, and commits itself to the peaceful use of cyberspace.

For instance, Glennon claims that "ensuring the safety of their residents is the core of the states' constitutional responsibilities," and because international law is both inefficient and ineffective in defending a state's members, "the best defense will therefore continue to lie not in international law but in national efforts to defend against them and mitigate their efforts. This is where states can play a pivotal role. They can take firm steps to prevent cyber-intrusions, monitor malicious traffic, mandate cybersecurity measures, and mitigate the effects of such intrusions when defensive safeguards fail."

II. BACKGROUND

Before going into detail of the stance difference between the U.S. and China, it is important to briefly mention how cybersecurity is defined in this paper, and how cybersecurity issues should be handled in the context of international relations. To date, there is no universal definition of cybersecurity. This is partly due to the fact that while it is a type of security issue, cybersecurity is more complicated than it appears to be. Cyber-attacks cannot be easily fit into existing concepts such as war or crime, and still it is a critical part of national security with a vast range of non-state actors involved. This chapter will therefore provide the backgrounds necessary to develop the following chapters.

1. What is Cybersecurity?

Recently, witnessing the rapid development of information technology and the new threats it entails, states and international organizations have recognized the need to address security issues related to the cyberspace. The critical infrastructure systems - which are used in water, public health, emergency service, energy, banking and finance sector - of most industrialized countries are managed by networked technology, which has made them vulnerable to cyber-attacks. Some recent cases such as the 2007 cyber-attacks on websites of Estonian organizations or the 2009 7.7 DDoS(Distributed Denial of Service) attack on South Korean websites have illustrated the weakness which stems from the openness and interconnectedness of the Internet and the cyberspace as a whole.

Against this backdrop, the Report of the Group of Governmental Experts has recognized the existence of information security threats relevant to international security. Some states have made efforts to consider 'Cybersecurity' as part of national security and initiated preliminary steps for multilateral collaboration in international and regional organizations. In order to combat cybercrime, which is transnational in nature, the Council of Europe has made efforts to facilitate international cooperation in cybercrime investigation by an international treaty called the Convention on Cybercrime. Consequently, the discussion on how to protect the cyberspace, or eliminate the threats from cyberspace, has been growing in the international arena, and will continue to grow as the number of cyber-attack cases increases.

Many researchers have already been motivated by the fact that policy issues involved in cybersecurity have significant impact on foreign relations and will continue to grow in importance. Given the open nature of the Internet, it is true that no state can handle the issue of cybersecurity single-handedly. Cybersecurity is by nature a truly global issue that requires cooperation and collaboration among both states and non-state actors, such as ISP companies. But still there remains a large area unexplored laid between international relations and cybersecurity. Research on cybersecurity and international relations in general is still in its infancy.

One critical case illustrating the need for future research in this area is the fact that even official consensus has not been reached on the basic definition of "cybersecurity", despite numerous attempts to do so. In 2005, International Telecommunications Union (ITU) has made one such attempt by comparing various national cybersecurity initiatives

in order to identify common themes and best practices. According to this document, "cybersecurity" refers to three things:

1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to national security;
2. The degree of protection resulting from the application of these activities and measures;
3. The associated field of professional endeavor, including research and analysis, aimed at implementing and those activities and improving their quality.

According to the concept of security put forward by David Baldwin, apart from this question of "Security from what threats?", questions such as "Security for whom?" and "Security for which values?" are also important components in distinguishing diverse perspectives and understanding different viewpoints among states regarding cybersecurity. For the purpose of this study, these three questions will be used in clarifying U.S. and China's perception on cybersecurity.

Simply put, "cybersecurity" is concerned with protecting cyberspace from "cyber-threats." As to how states specifically define cybersecurity and establish countermeasures, e.g., cybersecurity initiatives and policies, depends on how they understand cyber-threats. What this implies is that as long as there remains a huge gap between states' perceptions on threats and security regarding the cyberspace, further attempts to realize international cooperation in protecting the cyberspace from such threats may lead nowhere. In short,

the different ways in which states perceive what cybersecurity is will hinder the process of reaching a consensus on how states should coordinate.

Although an international agreement on the concrete definition of cybersecurity has not been reached, for the purpose of this study "cybersecurity" is defined as a set of activities and measures intended to protect "cyberspace" from " all threats", including threats to "national security" and "cybercrime", namely threats targeting private corporations and individual computer users, alike. Additionally, unlike traditional security issues which usually involves mostly state actors, the characteristics of the cyberspace itself requires the participation of both states and non-state actors in securing the cyberspace against existing and potential threats. The next section will discuss these points in detail.

2. Attributes of Cybersecurity and International Relations

a. Characteristics of Cybersecurity

1) Interdependence

Historically, the Internet was designed to facilitate access and utilization, rather than security. This inborn weakness of the Internet has been the source of insecurity for the cyberspace as a whole. Additionally, the absence of a single authority in charge of governing or securing the Internet has contributed to the complexity involved in securing it, because the Internet is a decentralized and open network of computer networks which

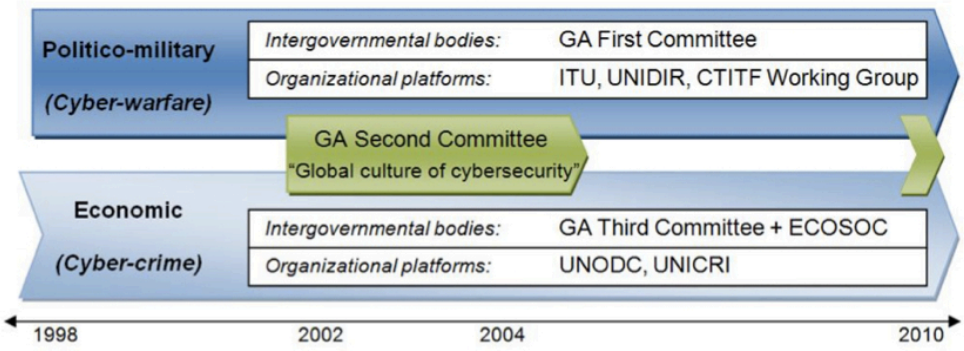
are subject to different territorial laws and policies. Thus, participation in international agreements and cooperation is indispensable in securing the cyberspace. Even the United States has officially recognized this need to participate, although for years it had been almost exclusively depending on unilateral measures to deter cyber-attacks. This shows the uniqueness of cybersecurity as a security issue: states must cooperate with each other in order to achieve security, since everything is connected.

2) Difficulty of Attribution

Another problem is the difficulty in distinguishing the specific types of cyber-attacks, which tends to blur the distinction among traditional concepts such as war and crime. The Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201) has acknowledged that the type of cyber-attacks range from criminal conducts such as the theft of money to inter-state conflicts such as warfare, but due to the nature of the cyberspace, it is difficult to attribute a certain attack to cybercrime or cyber-war. Traditionally, the regulation and deterrence of crime belongs to the purview of criminal justice and the perpetrator is punished by the law enforcement, which is mostly based on domestic law. On the other hand, warfare is conflict between states and follows the rules of international law. When physical attack was the only possible form of aggression, this dual approach and response was quite reasonable. But since stories of cyber attacks started to make the front page in all newspapers, it is becoming all the more difficult to conceptually distinguish between warfare and crime and decide how to resolve a certain

case.

Currently there are two main approaches which is common at both the national and international level when viewing cyber-attacks: a *security-oriented approach*, which first originated from viewing the threats from cyberspace as a technical threat to national security; and a *law enforcement approach*, which approaches the issue from a criminal justice point of view. The former has a tendency to focus on deterrence and prevention, while the latter emphasizes on investigation and attribution. This point is well identified in Maurer (2011)'s work. Maurer distinguished two streams of discourse in the United Nations on cyber security issues: the politico-military stream, which mainly has to do with cyber arms race; and the economic stream focusing on the criminal use of information technologies.



[Picture 1] Two Streams Model of Cyber Norm Emergence in the United Nations

While this Two streams Model shows how international norms of cybersecurity is currently emerging in the United Nations, in reality the line distinguishing cyber-warfare and cybercrime is not visible at all. The bigger picture of cyber-attacks in general has

blurred the traditional boundaries that existed between crime and warfare. Technically this is because it is difficult to trace the attacker, and easier for the attacker to disguise or detour. Other than technical reasons, there are legal problems in tracing information located overseas and difficulties in acquiring voluntary cooperation from foreign counterparts. Since a precise method for attribution has yet to be developed, the attribution process should be based upon several elements put together, such as the type of attack, subject, period of time, the size and impact of the attack, target of attack, and motive,. However, it is very difficult to collect all these information perfectly due to the distributed nature of cyber attacks and the lack of partnership among relevant organizations at the current stage. Given the difficulty of distinguishing between a cyber-attack that threatens national security and cybercrime, states have a tendency to tilt toward the security-oriented view.

On this point, Nye (2010) has classified four major cyber threats to national security as economic espionage, crime, cyber war, and cyber terrorism. These concepts are widely used, despite the fact that there is no universal definition for these concepts, which makes demarcation among them difficult. Nevertheless, basically all four concepts have one thing in common: they are all subject to the regulation of law. Cyber war should be ruled by international law, while cyber terrorism, cybercrime and economic espionage can be categorized as crime and is subject to criminal law. Since there is no fully developed international practice or norm regarding cyber war to date and both economic espionage and cyber terrorism can be classified as a type of cybercrime, there is no point in distinguishing between the type of legislation applied to each of the four attacks. Rather,

demarcation has a bigger meaning in practical terms such as deciding the division of labor among relevant organizations and agencies in response to such incidents.

Regarding criminal investigation, the discussion on the role in attribution is especially important. This point was already made by the United States in 2003 in The National Strategy to Secure Cyberspace:

> "Law enforcement and the national security community play a critical role in preventing attacks in cyberspace. Law enforcement plays the central role in attributing an attack through the exercise of criminal justice authorities. Many cyber-based attacks are crimes. As a result the Justice Department's Computer Crime and Intellectual Property Section, the FBI's Cyber Division, and the U.S. Secret Service all play a central role in apprehending and swiftly bringing to justice the responsible individuals. (...) Ideally, an investigation, arrest, and prosecution of the perpetrators, or a diplomatic response in the case of a state-sponsored action, will follow such an incident."

It is a natural corollary for the law enforcement to play the central role in attribution since legal authority prescribed by the criminal justice procedure is necessary in identifying the origin and thus attributing a cyber attack case to a certain type of attack, and because it is generally allowed to take a criminal justice approach regardless of the type of attack. Under normal situations, a case should be first attributed to a certain type through investigation led by law enforcement agencies in order to decide how to respond to it depending on its type of attack.

3) Discrepancies among States

However, the overall structure of cyber attacks response differs from one state to another, and some countries have cyber crisis management systems that put defense and damage restoration above cyber attack attribution. By doing so, it becomes extremely difficult not only in the attribution of a certain cyber attack, but also in generating information about the "changing nature of threats, the characteristics and methodologies of threats, and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention," which is critical for both the academic circle of criminology and decision-makers who establish national strategies for the cyberspace.

In fact, currently there are no methodologically sound international surveys which can measure cybercrimes, not only because there is no agreed-upon definition of cybercrime, but also because the information regarding cyber-attacks do not flow through a single channel. This contrasts the flow of information of traditional crime, which is usually reported to law enforcement agencies. Cases of cybercrime or cyber-attacks are sometimes reported to different governmental agencies or to the private sector, or not reported at all.

In short, the openness and interconnectedness of the cyberspace makes international cooperation fundamentally important in dealing with cybersecurity issues. Cybersecurity blurs the traditional distinction between war and crime, and it is evident that law enforcement plays a critical role in attributing a certain attack. However, as many states have already recognized cybersecurity as an integral part of national security, the lack of

agreement upon the categorization of cyber-attacks and certain definitions, and the difficulty of cyber-attack attribution further tilts states to take a security-oriented view on this issue, rather than the law enforcement approach.

b. Cooperation or Competition (or Conflict)?

Just as the several different approaches to international relations (e.g. realism, liberalism, and constructivism) available in analyzing international affairs hold very different views on how to solve a certain problem, the solution to cybersecurity problems may differ greatly depending on how the cybersecurity issue is initially framed. While the two approaches discussed above (security-oriented approach and law enforcement approach) originate from the discrete areas within the bigger frame of state sovereignty, the two approaches to be discussed here are mainly about framing cybersecurity in the long-standing topic of international relations: cooperation and competition (or conflict).

1) Cooperation?

International cooperation is one of the main research topics of international studies. Following Robert Keohane, 'cooperation' is commonly defined as occurring "when actors adjust their behavior to the actual or anticipated preferences of others, through a process of policy coordination." According to Milner, this definition of cooperation consists of two important elements. First, each actor's behavior is directed toward some goal(s), and second, it implies that cooperation provides the actors with gains or rewards.

When considering traditional security issues, many people have usually focused on questions such as: under what conditions cooperation was possible or not, or how to make a working peace system that deters warfare, centering on the relationship among states. This approach has a tendency to define security in terms of national security, which places the most emphasis on the role of states and their maintenance of state sovereignty against external military threats. The premise on which the concept of traditional security lies is that as long as a state's sovereignty is secure from external threats, consequently the security of individuals would be guaranteed. In this context, long-term international cooperation is based on the agreement states reach as a result of negotiations, which is usually codified into international treaties.

However, globalization and the end of the Cold War have brought new security challenges the global society faces today. Unlike traditional security issues in which states were the primary - sometimes the only - actors, these new security issues involve an array of non-state actions and a diversity of non-state actors, and thus can no longer fit into the premise on which the concept of traditional security is based. In the context of these new challenges, such as transnational organized crime and human/drug trafficking, genocide, trade disputes and pollution, the security of individuals can be threatened even when state sovereignty is secured from external military threat. If one holds on to this state-centered view of traditional security in understanding such current security problems, these new threats are bound to be overseen or only partly solved. This is because there is a tendency to conceptually limit the subject of security to the state when considering traditional security issues, while non-traditional security issues are in need of

a more comprehensive approach.

What makes non-traditional security different from traditional security are the following characteristics of it: first, it focuses on threats to *non-military* security; second, most non-traditional security issues are *transnational* in terms of its cause and effect; and third, it *includes non-state actors* as well as states when using the concept of security. These features of non-traditional security issues calls for a multilateral approach that includes all actors involved, state and non-state. Therefore, rather than holding on to the narrowly-defined paradigm of traditional security which mostly focuses on *international* cooperation, a more comprehensive concept of security and a *global governance* approach is needed in order to properly grasp the non-traditional security issues and find solutions to these problems. However, this does not mean that states are no longer important in solving non-traditional security problems. According to Lee(2008), the concept of non-traditional security still views states as a primary concern.

Based on the differences between the traditional security and non-traditional security issues, cybersecurity is a type of non-traditional security issue in that: 1) it blurs the distinction between military and non-military issues (such as cybercrime), 2) it is transnational in nature and its impact, and 3) it involves both states and non-state actors. Cooperation limited to states is insufficient in eliminating threats to the cyberspace, because private sector actors, such as internet service providers(ISP), are in charge of managing most of the infrastructure on which the Internet is based. As Chadwick(2006) has mentioned:

> "The politics of the Internet are played out in the interaction between states and citizens, public and private actors, in a variety of arenas, some of which do not even appear to be political - on the surface at least. (...) Governments and legal regimes cannot always deal with the implications of the Internet in the "command and control" modes of the past, though they will undoubtably try. Understanding the politics of Internet technologies - their usage, distribution, design, and regulation - requires us to think in terms of the diverse actors, new communities, interests, and interdependencies they foster."

This perspective of viewing cybersecurity as a non-traditional security issue is also supported by some Chinese scholars. Some of them (吕诚昭, 郝文江, 武 捷) have argued that cybersecurity and information security is directly related to national critical infrastructure, thus affects national defense, economic prosperity and basic everyday life conditions, and because no single state can solve cybersecurity problems alone, domestically a partnership between the public and private sector is needed; internationally cooperation is integral in governing cybersecurity problems. Specifically, they claim that cybersecurity problems entail attributes such as interdependency and anonymity, which strengthens the following general characteristics of non-traditional security issues: transnational nature, uncertainty, dynamism, and need for cooperation for resolution of the problem.

2) Comptetition (or Conflict)?

Indeed, cybersecurity is transnational in nature, and has more uncertainties and dynamism in itself compared to other traditional security issues, and it is reasonable to argue that cooperation is vital in both between the private and public sector as well as between and among states. However, while cooperation and collaboration among various actors involved in cybersecurity is *desirable*, it does not necessarily mean the reality will follow the ideal. In fact, while most states and non-state actors have all recognized and agreed on the need to cooperate, some still have suspicion towards the moves and intentions of other actors. Indeed, this kind of literature takes up a large proportion of prior research in both the U.S. and China.

For example, Manson (2011) has maintained that "If the United States and China find themselves in conflict in the coming decades, this newest arena of operations, cyberwarfare, will play a decisive role in determining the outcome."

In a similar sense, Jiang Yong (江涌) (2010) views the cyberspace as a place where major international competition is taking place, and winning this competition is critical to the comprehensive national power. The interesting thing is that both writers make their points by describing how their counterpart state (i.e. in Manson's perspective, China; in Jiang's perspective, the U.S.) is preparing for offensive use of cyber capability, while silencing or justifying their own country's stances.

Nevertheless, it is noteworthy to say that this tendency to emphasize competition rather than cooperation in cyberspace is, compared to the perspective discussed above which stresses the non-traditional security aspects of cybersecurity, is focusing more on

the ‘continuity’ of competition or conflict in international relations. In other words, while the perspective that places more importance to the non-traditional aspects of cybersecurity, such as the involvement of diverse actors other than the state in a security issue, leads to a need for cooperation and partnerships among involved actors, this perspective concludes by suggesting measures to strengthen cyber capabilities in order to successfully compete in the international stage.

However, cybersecurity is more complex and defies traditional classification and concepts. When talking about critical infrastructures and its function directly linked to providing people’s everyday life needs, and the deep involvement of Internet Service Providers in managing such facilities, cybersecurity may be classified as a non-traditional issue. In this case, the emphasis is on the increased role of non-state actors compared to that of traditional security issues, in which mostly states played the most important, and sometimes the only, role. On the other hand, if information technology is applied to traditional kinetic weaponry and military operations, or utilized in launching a cyberattack upon a state, it could also be part of a traditional security issue, in which the state still dominates the problem-solving process. At the current state of development of the cybersecurity discourse it is difficult to classify cybersecurity either as a non-traditional security issue or a traditional security issue, since it could be both. In some cases, states still maintain the primary role; but in other cases, states will have to prepare more space for non-state actors to participate.

This leads us to the question of the role of the state in dealing with security issues in the context of globalization. On whether or not the role of the state should be downplayed

(that is, due to the transformation of security issues by globlaization, Clark (1999) has argued that "the question that has to be addressed by the student of contemporary security is not whether security should be reconceptualized around individuals or societies as alternatives to the state, but how the practice of states is being reconfigured to take accounts of new concerns with human rights and societal identity." In other words, rather than focusing on whether the cybersecurity issue is a non-traditional security issue that shrinks the role of the state, or a traditional security issue which empowers the state to take the lead in strengthening its national capabilities to cope with cybersecurity problems, it is necessary to pay attention to how state agendas have been transformed, since "states are not withering away but are being transformed as they struggle to deal with the range of new challenges (including those of security) that face them."

Therefore, in order to gain deeper understanding on how to frame cybersecurity issues in the international context, it is both important and necessary to understand in what way states have transformed their agendas to cope with cybersecurity issues.

3. Cybersecurity: Mission Impossible?

But even for states, let alone non-state actors, it is difficult to come up with such international agreements. It took a long time for the Council of Europe to complete the Convention on Cybercrime, not only because of disagreements over hate speech, but because the investigation of crime belongs to the purview of national sovereignty. Many have States are sensitive about sovereignty and are not likely to relinquish it. Goldsmith and Wu (2006) have pointed out that "Even in the cybercrime context where there is

general consensus about the need for cooperation, it is very hard for nations to agree." They further mention the limits of international treaties (specifically the Convention on Cybercrime) and cooperation, and argue that:

> "(...) many Internet controversies are fast transforming into disputes among nations, and classic problems of international relations. Whether the issue is online gambling, Internet domain name governance, or privacy laws, (...) *governments are fighting one another to favor themselves, using the traditional tools of international politics and international law*."
> "This lengthy process [of the Convention on Cybercrime] is not unusual for any treaty, and especially one that requires international cooperation in a core area of national sovereignty. But the process is too long and unwieldy to effectively regulate cybercrime, a constantly changing threat that requires immediate national responses and international cooperation."
> "The failure of the cybercrime convention typifies the role that treaties have played in the Internet era. (...) *For the Internet, unilateral action, conflict, and ad hoc accommodation are often the best the nations of the world can do*."

According to the arguments of Goldsmith and Wu, it seems unreasonable for states to take part in cooperative initiatives of all kind, since "hard" cooperation based on the Convention on Cybercrime has "failed," and there has not been any other international treaties other than this. Because of the limited role international treaties can play in facilitating cooperation, states are more likely to engage in international conflicts by "using the traditional tools of international politics and international law." In this way Goldsmith and Wu places a bigger emphasis on the possibility of conflict, rather than that

of cooperation in cybersecurity issues. They even go as far as to claim that a "technological version of the cold war" might take place.

III. U.S.-China Stance Difference

As mentioned above, this section provides the perspectives of the United States and China on the issue of cybersecurity based on three main sources of material: the Report of the Secretary General in the United Nations First Committee, official government documents (white papers), and domestic literature and prior research by scholars in each country. While the official state opinions available from the Report of the Secretary General shows how the stances of the two states have evolved over time from 1998 to recently, the official government document represents how the two governments view this issue and prioritizes the most in terms of cybersecurity. Meanwhile, the domestic literature from both states provides an overview to what kind of opinions scholars have about cybersecurity issues, and how they view each other (in China's case, the United States; in the U.S.'s case, China). In order to understand the current stance difference between U.S. and China, this section starts from UN materials to show the evolution of the stances.

The "fragmented" cybersecurity discourse in the UN is well summarized in Maurer's work. According to Maurer, the debate on cybersecurity in the UN General Assembly First Committee was initiated in 1998 by Russia. The Letter from the permanent representative of the Russian Federation to the United Nations addressed to the Secretary-General, which was circulated in the First Committee, requests the United Nations to consider "the question of international information security to be a topic for substantive and purposeful discussion." Additionally, the Russian Federation introduced a

draft resolution that proposed the Member States to increase their considerations of threats at the bilateral and multilateral levels and invited them to inform the Secretary General of their views and assessments concerning cybersecurity issues, which was under the title of "Developments in the field of information and telecommunications in the context of international security." This initiated the works of the First Committee, which is well summarized in Tikk-Ringas (2012)'s policy brief. General Assembly resolution 53/70 had initially invited all Member States to inform the Secretary General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;
(b) Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources;
(c) Advisability of developing international principles that would enhance the security of global information and telecommunications systems to help to combat information terrorism and criminality.

Later, in resolution 55/28 the third question was revised as to "(c) The content of the concepts mentioned in paragraph 2 [relevant international concepts aimed at strengthening the security of global information and telecommunications systems] of the present resolution."

Among the statements which states sent to the Security General, this section analyzes those of the United States and China. The United States submitted statements in

1999, 2004, and 2011, and these statements grow in length as time passes. China has sent their opinions in 2004, 2006, 2007 and 2008. By examining the statements of both countries in sequential order, it is possible to understand how their perspectives have evolved over time. Three questions which Baldwin put forward in defining the concept of security, “Security from what threats?”, “Security for whom?” and “Security for which values?”, will be used as the criteria of comparison in this paper.

1. United States

a. The Report of the Secretary General (1999, 2004, 2011)

The following table summarizes the main points made by the United States in the report of the Secretary General in the UN General Assembly First Committee. The contents are categorized in the three questions which were used in Baldwin’s work.

	Security from what threats?	Security for whom?	Security for which values?
a) 1999 (A/54/213)	- Criminal or terrorist misuse of information technology - Unlawful intrusion or attempt to disrupt or alter any aspects of national information systems	- Many diverse activities of individuals, groups and governments - Critical national infrastructure - Intellectual property and protection of privacy - Protection of information related to military capabilities and other aspects of national security	- Sustaining interaction between states - Integrity of domestic information system - Reliability and safety from criminal misuse or denial of service

b) 2004 (A/59/116/ Add.1)	- Key threat to cybersecurity originates in the relentless criminal attacks by organized criminal, individual hackers and non-state actors, including terrorists	- The reliability, integrity and availability of national and global information infrastructure	- The principle of free flow of information (the freedom of any individual to seek, receive and impart information and ideas through any media)
c) 2011 (A/66/152)	- disrupt or alter any aspects of national information systems - State based/non-state actors' criminal or terrorist activity with varying motivations (from the theft of money or information, disruption of competitors, nationalism and extension of traditional forms of state conflict into cyberspace	- The reliable functioning of critical national (information) infrastructures, global networks and the integrity of the information that travels or is stored with them - Individuals, corporations, critical national infrastructures and governments	- The rights to freedom of expression and the free flow of information

Aside from the contents categorized above, other attributes noteworthy are as follows. In 1999, the U.S., while mentioning the use of both unilateral and multilateral means in order to unsure the integrity of domestic information system, also claimed that all states must take steps to review domestic statutes to provide ways to prosecute actions related to criminal or terrorist misuse of information systems. Unlike its attitude towards strengthening each states' capacity to combat the criminal misuse of information systems, the U.S. has been essentially against the attempt to make a new legal framework for information security. The U.S. has argued that, since information security is a complex topic that needs thorough analysis, it is premature to formulate overarching principles

pertaining to information security in all its aspects.

In 2004, the U.S. continued its argument against a new legal framework by openly criticizing the claims of some states that cybersecurity can be achieved by an international convention, in that this proposal implicitly implies the right of government to control information that is transmitted into national territory from outside of its borders, and this contravenes the principle of free flow of information. In addition, the U.S. claimed that with respect to military applications of information technology, an international convention is completely unnecessary, since the law of armed conflict and its principles of necessity, proportionality and limitation of collateral damage already govern the use of such technologies. Rather, the U.S. claimed that effective criminalization by states of the misuse of information technology and the creation of a global culture of cybersecurity can best protect the benefits of cyberspace, and that states should be encouraged to implement the eleven principles drafted by critical information infrastructure protection experts from G8.

In 2011, the stance of the U.S. developed considerably, compared to its reports of the past. While the U.S. still cling onto its strong opposition to the need for a new legal framework specific to cyberspace, it claimed that international collaboration on strategies to reduce risks to information and communications technologies is essential to ensure the security of all. It developed its reasoning against the claims for a new legal framework by outlining existing resolutions that could work as norms in cybersecurity issues: for example, the General Assembly resolutions regarding cybercrime (A/RES/55/63, A/RES/56/21), global culture of cybersecurity and the protection of critical information

infrastructures (A/RES/57/239, A/RES/58/199), and the resolution that invited all Member States to take detailed stock of their national cybersecurity efforts to date (A/RES/64/211), claiming that these resolutions advance some useful norms for individual and state behavior in the interest of cybersecurity. By pointing out the lack of shared understanding of international norms pertaining to state behavior in cyberspace which could affect crisis management in the event of major cyberevents, the U.S. implies a need for norms that are based upon existing international norms rather than a separate, obligatory international convention or legal framework for cybersecurity. Also, it mentioned that states should undertake both domestic and international tasks in order to address the transnational nature of the various threats. In addition, the U.S. recognized the unique attributes of ICT, such as the developing capabilities of non-state actores, involvement of the private sector in operating the networks that constitute cyberspace, which make traditional strategies such as measures similar to those used for arms control ineffective, and claimed that this leads to the need of creative new approaches to mitigate the risks. The U.S. also pointed out the difficulty of attribution of a cyber attack by mentioning that high-confidence attribution of identity to perpetrators cannot be achieved in a timely manner due to the attributes of the cyberspace, and success depends on a high degree of transnational cooperation.

In sum, in all three reports the United States has maintained its strong opposition against a new legal framework specific to cybersecurity, while continuously developing its argument by outlining the existing norms that can be applied to state behavior in cyberspace which can substitute the convention proposed by some states, such as China.

b. Government Official Document: <International Strategy for Cyberspace> (2011)

Overview

Unlike China, the United States does not devote a large part in describing and elaborating the threats they face in terms of cybersecurity. On the other hand, they seem to be more occupied with spreading the value of 'freedom' in the Internet, putting forward their ideas for the future of the Internet, and setting new norms and standards in regulating the cyberspace. Interestingly, as this paper was issued later than China's White Paper, it contains some statements seemingly aimed at criticizing China's policies . In addition, in this document the U.S. outlines its priorities and principles in terms of norms pertaining to state behavior in cyberspace.

Purpose

The introduction from President Obama introduces this paper as:

> "... it is the first time that our Nation has laid out ***an approach that unifies our engagement with international partners on the full range of cyber issues***. And so this strategy outlines not only a ***vision fo the future of cyberspace***, but an ***agenda for realizing it.*** It provides the context for our partners at home and abroad to ***understand our priorities,*** and how we can come together to preserve the character of cyberspace and reduce the threats we face."

Security from what threats?: ***Wide range of threats***

The U.S. government recognizes a wide range of threats:

> ***"Natural disasters, accidents, or sabotage (...) Technical challenges (...) Extortion, fraud, identity theft, and child exploitation (...) The theft of intellectual property (...) These challenges transcend national boarders."***

Security for whom?: ***Wide range of security subjects***

The U.S. also declares a wider range of security subjects, ranging from individual user security to international peace and security:

> "(...) cables, servers, and wireless networks on U.S. soil and beyond (...) international network disruption (...) ***user***'s confidence in online commerce, social networks and even their ***personal safety*** (...) ***national competitiveness*** and the innovation that drives it."
>
> "(...) strong cybersecurity is critical to ***national and economic security*** in the broadest sense, (...)"
>
> "Cybersecurity threats can even endanger ***international peace and security*** more broadly, as traditional forms of conflict are extended into cyberspace."

With the wide range of security subjects, the U.S. government stipulates the need for multi-stakeholder governance:

> "Internet governance efforts must not be limited to governments, but ***should include all appropriate stakeholders***."

Security for which values?: ***Freedoms, Free Flow of Information, Stability through Norms***

A large part of this document accounts for the principles and norms the U.S. government deems indispensable in leading the future of the Internet in their favor. While China stressed on respect for national sovereignty in cyberspace and suggests equality and mutual respect as the basis of international cooperation, the U.S. on the other hand highlights the value of freedom and the role of norms in maintaining stability and promoting international cooperation.

1) Core Principles

> "***Fundamental Freedoms***. (...) the ability to seek, receive and impart information and ideas through any medium and regardless of frontiers (...)"
>
> "***Privacy***. (...) individuals should be able to understand how their personal data may be used, and be confident that it will be handled fairly."
>
> "***Free Flow of Information***. States do not, and should not have to choose between the free flow of information and the security of their networks. (...)

2) Future of the Internet

> "The United States will work internationally to promote an ***open, interoperable, secure, and reliable*** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which ***norms of responsible behavior*** guide states' actions, sustain partnerships, and support the rule of law in cyberspace."

3) Stability Through Norms

> "The United States will work with like-minded states to establish an environment of expectations, or ***norms of behavior***, that ground foreign and defense policies and guide international partnerships. (...) We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace, with the understanding that an important first step in such efforts is applying the broad expectations of peaceful and just interstate conduct to cyberspace."

The basis for norms, in the view of the U.S. government, are the followings:

> "***Upholding Fundamental Freedoms*** (...) ***Respect for Property*** (...) ***Valuing Privacy*** (...) Protection from Crime (...) ***Right of Self-Defense*** (...) Global Interoperability (...) Network Stability (...) Reliable Access (...) Multi-stakeholder Governance (...) Cybersecurity Due Diligence (...)"

The explanation as to why the U.S. opposed cyber arms control, may be partially found in the following paragraph:

> "***We reserve the right to use all necessary means*** - diplomatic, informational, ***military***, and economic - as appropriate and consistent with applicable international law, ***in order to defend our Nation, our allies, our partners, and our interests***."

c. Domestic Literature on Cybersecurity in the U.S.

1) Evaluation of National Cyberspace Strategy / Approach to Cybersecurity

Right after the <International Strategy for Cyberspace> was released by the White House, Crook (2011) reviewed this Strategy along with the U.S. Department of Defense's security strategy for U.S. military networks. Although he did not explicitly comment on how U.S. cybersecurity strategy should look like or how this Strategy should be revised, he did outline the main points of them and especially emphasized strengthening norms affecting internet security.

Glennon (2012) outlined the current cybersecurity policy at the federal level, and by analyzing the utility of international law and other legal issues related to cybersecurity, concluded that states (in this case, states of the United States) can play a pivotal role in preventing cyber intrusion mitigating its effects. While it has come to be widely assumed that "cybersecurity is a federal responsibility" (p. 90), federal law and the federal government makes little or no meaningful effort to engage in mitigating the effects of cyber intrusions. He argued that states can fill in these gaps, or in some cases actually lead, for cybersecurity. In making his point, he mentioned the ineffectiveness of international law as a means to govern cybersecurity issues, and thus "national efforts to defend against [cyber intrusion] and mitigate their efforts" are the best defense.

Meanwhile, Maughan (2010) has furthered the discussion to what the U.S. must do in order to prepare for the time when the U.S. experiences cyberattacks daily and as global competition continues to increase. According to Maughan, the U.S. must

reenergize two key partnerships: partnership with the educational system in order to avoid a serious shortage of computer scientist/engineer/technologists; public-private partnership as well as international cooperation. In addition, he mentioned the Comprehensive National Cyber Initiative by the Obama administration: "The vision of the CNCI (Comprehensive National Cyber Initiative) research community over the next 10 years is to "transform the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances." Also, he emphasized the role of innovation: "It is only through innovative creation that the U.S. can regain its position as a leader in cyberspace."

In sum, while literature on this topic seems to be in abundance, these three works respectively summarizes the main points of the current cybersecurity policy in the U.S. and suggests measures the U.S. must take in order to "regain its position as a leader in cyberspace." The academic circle of the United States grasped the importance of strengthening norms, the ineffectiveness of international law and the role states can play to mitigate cyber incidents, and the need for a national cybersecurity research agenda that could further innovation and regain the leading role in cyberspace for the U.S.

2) Perception on China in the Cybersecurity context

Works related to U.S.-China relations in the cybersecurity context reveals how the academic circle in the U.S. perceive China. Apart from Liberthal & Singer (2012), in which the authors mostly introduced general knowledge about how the cybersecurity

realm works and what should be considered in the bilateral relation of U.S. and China, Manson (2011) and Melnitzky (2012) have both showed suspicion towards China's intention and the need for 'active defense' against China.

In <Cyberwar : The United States and China Prepare for the Next Generation of Conflict>, Manson examines the relative cyber strengths and weaknesses each country possess today by categorizing them into offensive capabilities, defensive capabilities, cyber dependence, Bejing's intentions, cyber events of Chinese origin (2005-2010), and difficulties of cyberattack attribution. While it is quite doubtful how one can distinguish between offensive and defensive capabilities in the cybersecurity context, since this realm lacks even the basic definition as to what cyberwar is, based on his work he shows suspicion towards the intention behind China's preparation. In doing so, the article mostly focuses on China's cyber espionage, and offers policy recommendations for the improvement of the U.S.'s own cyberwar capabilities. He concludes by proposing the U.S. to prepare itself in both offensive and defensive capabilities: "Either cyber-forensic capabilities must improve to such an extent that reliable counterstrike will come to mitigate first-mover advantage and nations will be deterred from attacking due to fear of the consequences and the expectation of international opprobrium, or cyberdefenses must become so robust that states do not anticipate any gain from the prosecution of cyber attack. The United States must prepare itself for both possibilities."

Meanwhile, in <Defending America Against Chinese Cyber Espionage Through the Use of Active Defense>, Melnitzky challenges the argument that cyber espionage must always be treated as a crime, as opposed to a national security threat. He argues that cyber

espionage, if pervasive enough, poses both a direct and indirect threat to national security. He asserts that "in response to this threat, the United States should employ what are known as "active defenses." An active defense is "effectively, a counter-cyberattack against the attacker's system, shutting down the attack before it can do further harm and/or damaging the perpetrator's system to stop it from launching future attacks."

3) On International Relations in Cybersecurity and Cyber Warfare

In <Cyberwar: The Future of Conflict>, Lifland briefly mentions Obama administration's cyberspace policies, and outlines the major issues involving the U.S. and U.K. on the one side, against countries such as Russia and China over the issue of whether a cyber attack should be recognized as a use of force against another nation and what the appropriate response to such intrusions should be. Like other authors she also recognizes the difficulty of attribution in case of a cyberattack as a reason for the difficulty in developing domestic and international legislation around cybersecurity issues. Nonetheless, she mentions the role of legislation in solving this issue: "the other legal issues face questions that must eventually be resolved through domestic and international legislation." While her work made some important points, such as the ongoing disagreement between the western countries and the SCO bloc, the title is a misnomer in that she does not mention much about cyberwar itself.

On cyber warfare itself, Krepinevich provides some insight by comparing cyber attacks with nuclear attacks in his work <Cyber Warfare: A "Nuclear Option"?>. According to Krepinevich, cyber attacks that would inflict catastrophic damage on critical

infrastructure is plausible and much more likely to occur than a nuclear attack, and the concerns over a cyber "Pearl Harbor" are legitimate. He gives several reasons as to why we are far more likely to experience major cyber attacks than nuclear attacks: the difficulty of attribution, proliferation of cyber weapons easier than nuclear weapons, and an absence of a clear cyber "firebreak," which clearly identifies the ambiguous nature of cyberspace and cyber attacks.

2. China

a. The Report of the Secretary General (2004, 2006, 2007, 2008)

The following table summarizes the main points made by China in each statement. It shows how the Chinese stance has evolved over time and what China views as the most important in the cybersecurity context.

	Security from what threats?	Security for whom?	Security for which values?
a) 2004 (A/59/116)	- Information criminality and terrorism	- International security	- International and regional peace, stability and development - United Nations Charter and other internationally accepted principles should be abided
b) 2006 (A/61/161)	- Risks arising from the weakness of the basic information infrastructure - The political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology	- The security of individual states and of the international community as a whole	- Information technology should be used in accordance with the Charter of the United Nations and the basic principles of international relations - The free flow of information should be guaranteed under the premise that ***national sovereignty and security must be safeguarded*** and that the ***historical, cultural and political differences among countries be respected***
c) 2007 (A/62/98)	- Risks arising from the weakness of the basic	- The general security of individual countries and	- Information technology should be used in

	information infrastructure - The political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology (*same from A/61/161)	the security and stability of the world as a whole	accordance with the Charter of the United Nations and the basic principles of international relations - The free flow of information should be guaranteed under the premise that ***national sovereignty and security must be safeguarded*** and that the ***historical, cultural and political differences among countries be respected*** (*same from A/61/161)
d) 2008 (A/63/139)	- The misuse of the products of computerization - Developing and using information weapons, information crime, information terrorism, using leadership in the information field to damage the interests and security of other countries, and ***disseminating information that undermines the political, economic and social systems and the spiritual cultural environment of other countries***	- Security and stability of individual countries and of the international community as a whole	- The political, economic and social systems and the spiritual cultural environment of other countries - The interest and security of states

Aside from the contents categorized above, other attributes noteworthy are as follows.

In 2004, China showed support for the establishment of the UN GGE(Group of

Governmental Experts) and claimed that use of information technology should abide by the United Nations Charter and other internationally accepted principles. In 2006, still upholding the United Nations as the "appropriate setting in which to resolve the problem of information security," China claimed that the problem of information security has already become a major factor influencing the comprehensive security of states and even global security and stability, thus the international community should share the responsibility. At the same time, it claimed that each state has the ***right to manage its own cyberspace*** in accordance with its domestic legislation

In 2007, China focused on listing its efforts, both domestic and international, to make the cyberspace a safer place. For domestic efforts, it claimed that China has drawn up and progressively implemented a national information-security strategy, and formulated a series of information-security laws, regulations and standard, and has strengthened network security monitoring, improving coordination and handling mechanisms, developing research on network-security technology, and constructing network-security emergency response systems. For international efforts, in June 2006 the heads of the member States of the Shanghai Cooperation Organization(SCO) signed the "Statement of the Heads of the member States of the Shanghai Cooperation Organization on international information security," in which it was decided to establish a group of experts on international information security. In addition, China claimed that the United Nations is the appropriate setting in which to explore the issue of information security, and that it supports the Group of Governmental Experts in carrying out a deep and comprehensive study of the threats and challenges in the field of information security.

In 2008, China remained consistent with its claim that the United Nations is the appropriate setting in which to explore the issue of information security, and claimed to support the reconvening by the United Nations in 2009 of the Group of Governmental Experts. It also claimed that China's public security agencies have established close cooperation and investigation assistance mechanisms with the police authorities of many countries.

In sum, China has continuously upheld the United Nations as the appropriate stage to have discussions about cybersecurity (although it still uses 'information security' as the main concept). China's claim that the right of each state to manage "its own cyberspace" seems to extend the notion of sovereignty into the cyberspace, as it has listed "the dissemination of information that undermines the political, economic and social systems and the spiritual cultural environment of other countries" as a major threat.

b. Government Official Document: <中国互联网状况> (2010)

Overview

This official document issued by the Chinese government, unlike that of the U.S., devotes a large part in describing the type of threats they face in cyberspace, and subsequently mentions "Internet sovereignty", which justifies governmental regulation on the Internet in China and defies the interference of other states. In addition, in maintaining support for a more democratic international order in 'Internet resource allocation,' implies Chinese government's opposition against the status quo in which the U.S. still has control of the root authority in the domain name system (DNS).

Purpose

"发表《中国互联网状况》白皮书，旨在介绍中国的互联网发展的基本情况，说明中国政府关于互联网的基本政策以及对相关问题的基本观点，帮助公众和国际社会全面了解中国互联网发展与管理的真实状况。(This white paper introduces the facts of the Internet situation in China, and elaborates on ***China's basic policies on the Interent and basic views on relevant issues***, thereby providing an overall picture to the Chinese people and the peoples of the rest of the world of the true situation of the Internet in China.)"

Security from what threats?: ***Dissemination of illegal information online***

While also recognizing other threats such as hacking and computer viruses, pornography and gambling, probably the biggest threat in the views of the Chinese government seems to be the dissemination of illegal information online.

"主张合理运用技术手段遏制互联网上违法信息传播。(China advocates the rational use of technology to curb ***dissemination of illegal information online***.)"

They even stipulate the contents that are banned from being produced, duplicated, announced or disseminated in detail.

Security for whom?: ***State security (Internet sovereignty), public interests and minors***

"中国政府主张依据相关法律法规，参照国际通行做法，发挥技术手段的防范作用，

遏制违法信息对国家安全、社会公共利益和未成年的危害。(The Chinese government advocates the exertion of technical means, in line with relevant laws and regulations and with reference to common international practices, to ***prevent and curb the harmful effects of illegal information on state security, public interests and minors.***)"

The Chinese government views the Internet as a national asset:

"中国政府认为，互联网是国家重要基础设施，中华人民共和国境内的互联网属于中国主权管辖范围，中国的互联网主权应受到尊重和维护。中华人民共和国公民及在中华人民共和国境内的外国公民、法人和其他组织在享有使用互联网权利和自由的同时，应当遵守中国法律法规、自觉维护互联网安全。(The Chinese government believes that the ***Internet is an important infrastructure facility for the nation***. ***Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected***. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, ***they must obey the laws and regulations of China and conscientiously protect Internet security.***)"

The interesting thing is that "Internet sovereignty" sounds very much like "cyberspace sovereignty" mentioned in Wu's 1997 work, but is the complete opposite. While "cyberspace sovereignty" was against state regulation on cyberspace, "Internet sovereignty" asserts state's right to regulate the Internet within its borders.

Security for which values?: ***Stability (safety), Respect for Difference, Equality and Mutual Benefit***

1) Safe flow of Internet information

> "维护互联网信息的安全流动。(...)应在保障互联网信息安全流动的前提下，实现互联网信息的自由流动。中国政府高度重视维护互联网信息的安全流动，积极引导人们依法办网、文明上网、正确用网。(Secure information flow. (...) ***On the premise of protecting the safe flow of Internet information, the free flow of the Internet information may be realized***. The Chinese government attaches great importance to protecting the safe flow of Internet information, actively guides people to manage websites in accordance with the law and use the Internet is a wholesome and correct way.)"

2) Respect for Difference

China especially emphasizes on the differences among states.

> "各国国情和文化传统不同，对互联网安全的关切也有差异，应充分尊重各国对互联网安全的不同关切，在差异中求和谐，在交流中促发展，共同维护国际互联网安全。(National situations and cultural traditions differ among countries, and so concern about Internet security also differs. ***Concerns about Internet security of different countries should be fully respected. We should seek common ground and reserve differences***, promote development through exchanges, and jointly protect international internet security.)"

3) On International Cooperation: Internet Sovereignty, Equality and Mutual Benefit

China seeks to connect the necessity of international cooperation in cybersecurity with its view of the Internet as an inevitably bordered world with multiple "Internet sovereignties" coexisting.

> "各国互联网彼此相联，同时又分属不同主权范围，这决定了加强国际交流和合作的必要性。中国主张，各国在平等互利的基础上，积极开展互联网领域的交流与合作，共同承担维护全球互联网安全的责任，促进互联网健康有序发展，分享互联网发展的机遇和成果。(Though connected, the ***Internet of various countries belongs to different sovereignties, which makes it necessary to strengthen international exchanges and cooperation in this field***. China maintains that all countries should, ***on the basis of equality and mutual respect***, actively conduct exchanges and cooperation in the Internet industry, jointly shoulder the responsibility of maintaining global Internet security, promote the healthy and orderly development of the industry, and share the opportunities and achievements brought about by this development.)"

> "各国应在平等互利的基础上开展多形式、多渠道、多层次的交流与合作。各国政府可建立双边交流机制，(...) 平等协商解决分歧。(...)
> 面对日益突出的瓜果网络犯罪问题，各国执法机构应加强共同防止和打击网络犯罪的侦查协作，建立多边或双边的合作机制。(All countries should conduct multi-form, multi-channel and multi-level exchanges and cooperation in this regard on the ***basis of equality and mutual benefit***. Their governments can establish bilateral exchange mechanisms, (...) and ***settle differences through consultations on an equal footing***. (...) In the face of the increasingly serious problems of transnational network crimes, the law enforcement agencies of all countries should enhance their coordination in preventing and

combating network crimes, and establish multilateral or bilateral cooperation mechanisms.)"

Especially, the following statement seems to show the Chinese government's dissatisfaction on the current domain name allocation system:

"中国认为，各国都有参与国际互联网基础资源管理的平等权利，应在现有管理模式的基础上建立一个多变的、透明的国际互联网基础资源分配体系，(...) (China maintains that ***all countries have equal rights in participating in the administration of the fundamental international resources of the Internet***, and a multilateral and transparent allocation system should be established on the basis of the current management mode, (...))"

c. Domestic Literature on Cybersecurity

1) Evaluation of National Cyberspace Strategy / Approach to Cybersecurity

In《我国国家网络空间安全战略的理论构建与实现路径 (The Theoretical Construction and Realization Path of State Cyberspace Security Strategy in China)》, Hui Zhibin (惠志斌) provided a systematic explanation of the origins of the theoretical background of China's national cyberspace strategy and suggests an ideal type of a national cyberspace security strategy model. According to Hui, cyberspace security has already become a part of the national security strategy. The state must mitigate and eliminate threats to national security in cyberspace, such as information warfare between states, infiltration by other states, the dissemination of indecent culture, terrorism and transnational crime, threats to the information system of critical industries, to list a few.

What is noteworthy in this work is that the author perceives (and claims that) the state as the central actor in securing the cyberspace. Not only does the author start from discussing cybersecurity as a critical component of national security, but also all the recommendations proposed in this work is state-centered: establishing a 'scientific' legal system for cyberspace security; pushing forward standardization for cyberspace security; and optimizing the organizational management system and strengthen human resources for cyberspace security.

Another author, Fang Qingtao (方清涛), focuses on information security, which is not exactly same as 'cybersecurity' but is deeply related. In fact, it is the concept which China uses frequently in SCO meetings and also in the Report of the Secretary General. In《中国国家信息安全与策略研究(A Study on China's Information Security and Measures)》, Fang argues that the biggest security problem is information security, and establishing economic/political/military/social/technological/cultural security on the basis of information security. According to Fang, information security is an important part of national security which has direct impact on a state's political stability, social stabilization, and a strategic point for economic development. He points out that competition surrounding information sovereignty and information resources have become a critical issue of national security in the era of information.

Meanwhile, Cheng Lin (程琳) has emphasized the need for a legal framework in dealing with cybersecurity issues. In《依法保障信息网络安全 (Internet Network Security Based on Law)》, he starts by listing the challenges China has come to face in

terms of cybersecurity, such as: intentional damages by utilizing psychological tactics by the cyberspace from western countries; espionage; and increasing amount of cybercrime and intrusion. He calls for the need to establish, use, and manage the cyberspace by law (依法建网、依法用网，依法管网), thereby securing national network sovereignty, cybersecurity order, resolving disputes in the cyberspace and strengthening governance and monitoring over the cyberspace. He also points out the problems current Chinese legislation on cyberspace has, and offers policy recommendations, such as: upholding network sovereignty and on its basis establish a legal framework for cyberspace legislation; strengthen law enforcement and improve the legal mechanism of governing cybersecurity; strengthen cybersecurity culture and implement 'rule of cyber law (网络法治意识)'; while retaining the strategic approach, push ahead international cooperation based upon legal structures (推动网络法治建设的国际合作).

2) Perception on U.S. in the Cybersecurity context

Yi Wenli (奕文莉) in《中美在网络空间的分歧与合作路径 (The Course of Conflict and Cooperation between China and U.S. in the Cyberspace)》outlined the conflict between U.S. and China in the cyberspace over topics such as "Internet Freedom" and internet/network sovereignty, internet governance, hacker attacks and competition in cyber military capacity, reflects the political, strategic and military conflict, and claimed that this in turn influences the bilateral relationship of U.S. and China. According to Yi, on the basis of building a 'new pattern of relationship between great powers

(新型大国关系) and new norms for the international cyberspace, China and the U.S. must strengthen bilateral communication, actively cooperate in areas of combatting cybercrime and promoting internet governance, and at the same time make efforts to reach mutual understanding and concessions in internet sovereignty and arms limitation.

Another author, Cai Cuihong (蔡翠红), furthers the discussion to areas in which competition between the U.S. and China have been triggered
In《网络空间中的中美关系 (China-U.S. Relations in the Context of Cyberspace)》, Cai argues that cyberspace has not only impacted the traditional relationship between the U.S. and China, but also has triggered the competition between the two, in areas such as cyberspace governance, strategic superiority, technological predominance, cyber arms race and discourse power (话语权). The most fundamental reason for this collision, according to Cai, is the conflict between China's internet sovereignty and U.S.'s interoperability of the internet. At the same time, the two states also cooperate on issues such as cybercrime, technological cooperation, etc. Cai proposes that while avoiding a security deadlock, China must pursue internet sovereignty and build a strategic partnership.

Liu Boran (刘勃然) and Huang Fengzhi (黄凤志) has analyzed the United States' 'International Strategy for Cyberspace'. In《美国'网络空间国际战略'评析 (An Analysis on the United States' 'International Strategy for Cyberspace')》, they claim that the U.S. has already placed cybersecurity as a new realm of international strategy, which insinuates that the U.S. is pursuing cyberspace hegemony as its objective.

As this has profound impact upon the new revolution in international strategy and has influenced the collision between values of cyberspace, it is both important and necessary to analyze and think about its influence upon U.S.-China relations and how China should respond to this new challenge.

Wang Gengxi (王更喜) goes further into casting a suspicious look to the intention of the U.S. In《美国输出价值观的新 "武器"(The United States using Values as a new "Weapon")》, Wang argues that U.S. public diplomacy, which views ensuring national security and national interest as the utmost priority, has been using its "norms" as a weapon to interfere in the domestic politics of other countries through cyberspace devices. According to Wang, this can be seen as an action of cyber "unilateralism," in which the U.S. is threatening the national security of another country in order to achieve its goals of national security and pursue its own interest. Wang claims that the political unrest in Middle East countries ("Arab spring") is a case that illustrates this point very well.

3) On International Relations in Cybersecurity and Cyber Warfare

Li Dayang (李大阳) in《浅析信息时代国际网络安全形势与我国对策 (A Brief Analysis on the situation of international cybersecurity in the information era and Measures for China)》claims that cyber warfare has become the new mode of conflict among states, and thus cybersecurity issues have become very important in considering national security. China has recently built up a new cyber unit and has put in place the "Great Wall of Cyberspace (网上长城)" in order to safeguard the state's

information territory. However, against the threats of cyber hegemony from western developed states, Li claims that China still has to make continuous efforts to improve its capacity in all aspects, including technology, management and international cooperation, in order to ensure national cybersecurity.

Written by a Chinese air force general Ma Xiaotian (马晓天), 《网络安全离不开国际合作 (Cybersecurity cannot be detached from international cooperation)》 is more focused on the need for international cooperation. Ma suggests four recommendations for building a "harmonious cyberspace": 1) joint establishment of cyberspace regulations; 2) strengthen international cooperation in combating cybercrime; 3) accelerate the development of cyber defensive technology; and improve the discussion mechanism regarding cybersecurity.

On the other hand, Jiang Yong (江涌) in《网络－看不见的战线 (The Cyberspace as an invisible Battlefield)》 views the cyberspace as an area for competition rather than cooperation. Jiang lists the uncertainties and ambiguities that stems from several aspects of cybersecurity, and mentions the recent increase in cyber attacks, and then turns to the claim that the United States holds the biggest and strongest, and the most developed cyber offensive capacity. Wang also assesses the intention behind the movements of the U.S. as to regain cyber hegemony and to take the advantageous point of reaping economic prosperity.

Shen Yan (申琰) in《互联网的国际博弈与合作研究 (On International games and international cooperation in the Internet)》 puts forward and support the concepts of

information sovereignty (信息主权), information security (信息安全), cybersecurity (网络安全), and information power (信息实力). By analyzing the impact of the Internet on politics, military, economy, science and technology, culture, and the international cyberspace order, Shen concludes that the Internet functions as a facilitator of competition and international games, while also increasing the possibility of international cooperation among states. Shen also offers policy recommendations based on an analysis of the status of China's 'power' in the Internet context.

3. Analysis of the Stance Difference

a. Evolution of Stances

Throughout the years, the United States has been continuously emphasizing the criminal side of threats to cybersecurity. The U.S. seems to be mostly concerned of the security of critical infrastructures, and since 2004 has been a strong advocate of the principle of free flow of information. On whether a new legal framework specific to cyberspace is necessary to achieve cybersecurity, the U.S. has maintained strong opposition and has continuously argued that existing principles of international law and UN General Assembly resolutions are sufficient to provide some useful standards for

state responsibility. But regarding the need for international norms for cyberspace, the U.S. initially refrained from discussions on formulating overarching principles pertaining to ***information security*** in all aspects, claiming that information security is a complex issue which needs thorough analysis. In 2004, the U.S. suggests that effective criminalization of states at the domestic level and the creation of a global culture of cybersecurity (which was adopted as a resolution in the General Assembly in 2002) at the international level will best serve the interests in pursuing cybersecurity. The most recent statement goes further to mention the lack of shared understanding of international norms pertaining to state behavior in cyberspace.

It is interesting to note here that the United States used the word "information security" in its 1999 statement, but changed the term into "cybersecurity" in 2004. In an article written in 2011, which deals with the International Code of Conduct for Information Security proposed by China, Russia, Tajikistan and Uzbekistan, Adam Segal explained the concept of information security as "includ[ing] not only the protection of computer, communication, and other critical networks that is the primary focus of U.S. officials, but also the threats that the free flow of information can present to domestic stability in closed authoritarian states." As to why the U.S. stopped using the term "information security" and turned to "cybersecurity" instead is out of the scope of this paper, but it is interesting to see how the U.S. is using a concept which itself once used in official statements to indirectly criticize the SCO bloc's Internet regulations.

Regarding international cooperation for cybersecurity, in 1999 the U.S. mentioned the use of unilateral measures as well as multilateral means in order to ensure the

integrity of domestic information system. Instead of stressing the need for transnational cooperation, in the early stage of the work of the First Committee the U.S. encouraged other states to review their respective domestic statutes and criminalize the misuse of information technology. This stance slightly changes in its statement of 2011, in which the U.S. recognizes the transnational nature of threats to cybersecurity and the difficulty of attributing cyber-attacks to certain perpetrators, which makes it no longer possible to apply the traditional strategies in resolving traditional security issues to cybersecurity. Although it still holds the need for states to conduct domestic tasks as well as international tasks, the U.S. now recognizes the attributes of cybersecurity issues which cannot be resolved without a high degree of international cooperation.

The initial stage of the evolution of China's perception on the threats to cybersecurity was similar to that of the U.S.'s: information criminality and terrorism. However, in 2006 and 2007 China claimed that the threats to information security arise from the inborn weakness of networks and the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology, and that each of these two factors is worthy of equal concern.

In 2008, China not only mentioned the threats posed by the misuse of computerization, but also brought forward the development of information technology for military use, the use of leadership in the information field to damage the interests and security of other countries, and the dissemination of information that undermines the political, economic and social systems and the spiritual cultural environment of other countries. This perception runs in the exactly opposite direction of the U.S.'s, which placed the free flow

of information as the priority value in pursuing cybersecurity. Moreover, while the U.S. did not mention the development of information technology for military use as a potential threat to cybersecurity, China has made it explicit that it is officially viewed as a threat to information security.

On international cooperation, China has been supporting the need to share the responsibility and cooperate for cybersecurity, viewing it as a problem that has become a major factor influencing global security. China has consistently claimed that the United Nations is the appropriate setting in which to launch discussions and explore the issue of information security, and showed support to the Group of Governmental Experts to examine the issue.

Just as the U.S. regards the free flow of information and freedom of expression as a fundamental value that should be protected, China has argued that national sovereignty and security must be safeguarded, and that historical, cultural and political differences among countries should be respected. Regarding sovereignty, China has also claimed that each state has its own right to manage ***its own cyberspace*** in accordance with its domestic legislation.

b. The "Red" Lines

Comparing the various materials, ranging from UN documents to government announcements and prior research of domestic scholars in both countries, it seems to be that "Red Lines," or discrepancies between U.S. and China seems indisputable. At the same time, the mutual suspicion illustrated in the domestic literature of both states seems

to exacerbate the deep divide between the two; yet both sides recognize that they cannot be free from the threats from cyberspace without international cooperation.

Among the many threats to cybersecurity, where these two states put emphasis on is different, and it holds the same for the scope of security subjects each state defines, with China focusing more on state security and public interest, while the U.S. defines the scope far more widely by even mentioning 'international peace and security'.

On the flow of information on the Internet, while China advocates national sovereignty and non- interference in the Chinese government's control of dissemination of "illegal information," the U.S. defines the "free" flow of information as a "fundamental freedom".

The basis for international cooperation in securing cyberspace is also different for these two states. China claims that the necessity for international cooperation stems from the fact that the "Internet of various countries belong to different sovereignties", demands respect for difference in national policies on cybersecurity, and views equality and mutual respect as the core principle in promoting international cooperation. Also, they insist that countries should "seek common ground and reserve differences." U.S., on the other hand, calls for "stability through norms," devoting itself in building a consensus on what constitutes acceptable behavior, and sets out its own ideas of what kind of norms the cyberspace should be regulated with.

While China indirectly criticizes the current domain name allocation system, in which the U.S. has physical control to the root, U.S. openly condemns governments that are seeking to exercise traditional national power through cyberspace and enhance

political control.

Regarding the role of the Internet, both states have recognized its importance in everyday life and economic prosperity. However, there is a stark contrast in the values they prize the most. China views the Internet as an important infrastructure facility for the nation, thereby justifying "Internet sovereignty" and governmental control in curbing dissemination of illegal information. The U.S. also mentions that "the underlying digital infrastructure is or will soon become a national asset", but also states that "States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure".

Whether the U.S. and China will be able to fill in these gaps to reach an agreement is unclear at the moment, and bilateral dialogue between the two states have just begun. For the time being, enhancing transparency and confidence building may help relieve the tension to some extent, but it cannot resolve the fundamental stance difference between the two without some kind of concession made by both states.

c. Summary of Analysis

As mentioned above, in this section the stance difference between U.S. and China will be analyzed against the three criteria from Abbott & Snidal's work, namely high sovereignty costs, uncertainty due to recentness, and degree of divergence among state preferences and capacities.

High Sovereignty Costs. Although expressed differently, both U.S. and China have

shown profound interest in securing the cyberspace as part of national security. The U.S. has continuously shown opposition towards forming a new legal framework specific to cyberspace, and instead called for 'norms' to regulate state behavior in cyberspace, of which most of them are existing international norms. This means that the U.S. has no interest in binding itself to a new international convention, and thus compromising part of its sovereignty. Instead, the U.S. has claimed that all states should strengthen their domestic law related to criminal misuse of information technology in order to effectively criminalize cybercrime. China, on the other hand, has developed a concept called 'Internet sovereignty (网络主权)' which justifies the Chinese government's right to control the Internet in China by making it part of its national sovereignty. Most Chinese scholars have argued that international cooperation is necessary, but only on the basis that Internet sovereignty is guaranteed. Both states seem to have a firm stance on this issue, which makes it difficult to find a common standing place for concession and agreement.

Uncertainty. The biggest uncertainty lying under the stance difference between U.S. and China is that so far there is no agreed upon definitions for cybersecurity, and due to the difficulty of attributing a certain attack and anonymity of cyberspace, this uncertainty leads to increased suspicion. While the U.S. started using 'cybersecurity' as the main concept, China is still promoting 'Information security', which makes one wonder whether the two states are on the same topic. Because no one can clearly distinguish whether a certain cyber attack against government websites or national infrastructure is a cybercrime or cyberwar, and cyber offensive or defensive capacities are

usually not open to public, states wearily eye each other and have a tendency to overestimate the capacity of its counterpart.

Degree of Divergence. As discussed above, both states acknowledged the need to cooperate in order to solve cybersecurity problems, but have fundamentally different priorities in terms of the value each prefer. The U.S. has stipulated 'free flow of information' as one of the principles it will pursue, while China has maintained that the 'safe flow of information' should be ensured on the basis of 'Internet sovereignty' or 'network sovereignty', and each state has the right to control its own cyberspace. It certainly looks difficult to bridge this deep gap, since both states have declared that it is their 'fundamental principle'. As to capacity, since both states perceive this issue critical to national security there currently is no reliable data to analyze the cyber capacity of both states, but based on the domestic literature review from both states, they are throwing suspicious looks to its counterpart. U.S. is accusing China of cyber espionage and its intentions and at the same time indirectly criticizing the Chinese government's control over the Internet in China, while China openly criticizes the U.S. that it is using its powers to maintain hegemony in cyberspace, and that it is using its "norms" as a weapon to interfere in the domestic politics of other countries through cyberspace devices. This mutual suspicion cannot be solved unless both counterparts start to strengthen bilateral or multilateral talks and try to narrow the stance difference.

IV. CONCLUSION: IMPLICATIONS FOR INTERNATIONAL COOPERATION

International cooperation, regardless of all fields, is essentially a result of the interplay between international politics and international law. Long-standing international cooperation is possible by binding agreements codified as international law, but states do not commit themselves to international agreements before deciding to adjust themselves to such arrangements, and whether or not states will bind themselves to international law is usually decided by the outcomes of political negotiations.

Building on the limits of hard law in facilitating international cooperation for cybersecurity pointed out by Goldsmith & Wu, the examination of the attributes of cybersecurity issues, and literature review on the role soft law can play in international relations, this paper has tried to identify the major factors that should be considered regarding international cooperation for cybersecurity issues. The state-centered traditional approach to security issues cannot bring effective outcomes when applied to cybersecurity issues, because cybersecurity involves both state and non-state actors, and the information infrastructure is usually managed by the private sector, which is why a global governance approach is more appropriate. However, states are still the major actors within the cybersecurity realm, and they are acting as the main norm entrepreneurs in the process of cyber norm emergence taking place in the United Nations, and now many states perceive cybersecurity as critical to their national security. Based on the works of the UN General Assembly First Committee from 1999 to 2012, it is expected that issues related to state responsibility and sovereignty will become the focal point of

the third GGE discussions. Therefore, the divergence in preferences among states on cybersecurity may greatly influence further developments in this field.

Among all states, the United States and China are undoubtably the two most important and influential actors in international relations. At the same time, the two states hold very different views on how the cyberspace should look like and be governed. Although many have noted the existence of this stance difference, works dedicated to this specific issue is scarce. By analyzing the stance difference of U.S. and China on this issue, this paper has shown that cybersecurity requires high sovereignty costs to both - for the U.S. it is because the U.S. views it as a critical part of its national security, while China has consistently supported the right of each states to regulate 'its own cyberspace' by its own domestic legislation - and that the uncertainty and complexity of the issue prevents both from starting costly and long negotiations that precede international agreements in the form of hard law. Most importantly, by contrasting the stances U.S. and China holds regarding cybersecurity, this paper has shown in which aspects and to what extent the two states differ in their perspectives. As mentioned above, participating parties in the negotiation process should know their counterparts' perspectives and how much it is different from their own perspective in order to find less sensitive issues to start the negotiating process with. Following prior research on the role of soft law, this may lead the cybersecurity discourse to international cooperation based on international arrangements in the form of soft laws.

BIBLIOGRAPHY

[한국]

강희종. “한국, 초고속 무선인터넷 보급률 ‘OECD 1위’.”디지털타임스. Published electronically July 5, 2011. http://www.dt.co.kr/contents.html?article_no=2011070502019931673002. (Last accessed: June 13, 2012)

김상배. 2007. “정보혁명과 안보환경의 변화: 한국군에 주는 시사점,” 한국사회과학 통권 제29권.

방송통신위원회 등. 2011. “2011 국가정보보호백서”, http://isis.kisa.or.kr/

방송통신위원회 블로그. 2011. “정부, <국가 사이버안보 마스터플랜> 수립,” http://blog.daum.net/kcc1335/3736 (Last accessed: May 30, 2012)

서동주. 2008. “한국정치학에서 ‘사이버 공간-안보’ 연구동향과 정책적 함의,” 국가전략 제14권 2호.

신봉수. 2007. “국제규범에 대한 중국의 전략적 사회구성: 주권, 민주주의,” 한국정치학회보 제41집 제3호.

____. 2006."중국적 규범(Norm)의 모색과 한계: 주권(Sovereignty)을 중심으로." 국제정치논총 제41집 제4호

이강규. 2011. “세계 각국의 사이버 안보 전략과 우리의 정책 방향-미국을 중심으로,” 방송통신정책 제23권 16호.

이신화. 2008. “비전통안보와 동북아지역협력,” 한국정치학회보 제42집 제2호.

정보라. 2012. 세계 인터넷, 정부 통제 시대 열리나. Bloter.net.

[中文]

马晓天. 2012. 5. 30. 网络安全离不开国际合作, 人民日报海外版.

谭安芬. 2011. 美国信息安全政策发展及其启示. 计算机安全.

蔡翠红. 2012. 网络空间的中美关系：竞争、冲突与合作. 美国研究, 3.

程琳. 2012. 10. 25. 依法保障信息网络安全, 光明日报.

申琰. 2009. 互联网的国际博弈与合作研究. (博士), 中共中央党校.

王更喜. 2012. 美国输出价值观的新“武器”. 中国教育报 理论周刊.

汤陈剑. 2011. “要强化国民的网络主权意识.” 当代社科视野, pp. 120-21.

江涌. 2010. 网络－看不见的新战线. 求是杂志, 13.

李鸿渊. 2008. “论网络主权与新的国家安全观,” 行政与法, pp. 120-22.

朱玉明. 2006. 论国家安全中的网络安全. (硕士), 湘潭大学.

曹鹏. 2008. 互联网对中国的国家主权的冲击及其维护策略. (硕士), 东北大学.

方清涛. 2009. 中国国家信息安全与策略研究. (博士), 河北师范大学.

惠志斌. 2012. 我国国家网络空间安全战略的理论构建与实现路径. 中国软科学, 5.

奕文莉. 2012. 中美在网络空间的分歧与合作路径. 现代国际关系, 7.

吕诚昭, 郝文江, & 捷, 武. 2012. 网络安全的非传统安全特征决定及其管理模式. 信息安全与通信保密.

卓翔. 2004. 网络犯罪若干问题研究. (博士), 中国政法大学.

刘勃然, & 黄凤志. 2012. 美国《网络空间国际战略》评析. 东北亚论坛, 3.

中华人民共和国国务院新闻办公室. 2010. “中国互联网状况”, http://www.gov.cn/zwgk/2010-06/08/content_1622866.htm

[English]

Abbot, Kenneth and Snidal, Duncan. 2000. “Hard and Soft Law in International Governance,” *International Organization*, 54, 3, pp. 421-456,

Baldwin, David. 1997. “The Concept of Security,” *Review of International Studies,* 23, pp. 5-26

Baylis, J. 2001. International and Global Security in the Post-Cold War Era. In J. Baylis & S. Smith (Eds.), The Globalization of World Politics: An Introduction to International Relations. Oxford and New York: Oxford University Press.

Betz, D. 2012. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. Journal of Strategic Studies, 35(5).

Carter, David L., and Joseph A. Schafer. "The Future of Law Enforcement Intelligence." In Policing 2020: Exploring the Future of Crime, Communities, and Policing, edited by Joseph A. Schafer: Police Futurists International.

Chadwick, Andrew. Internet Politics: States, Citizens, and New Communication Technologies. Oxford University Press, 2006.

Clarke, Richard, and Rob Knake. 2010. “Cyber War: The Next Threat to National Security and What to Do About It,” HarperCollins

Condron, Sean M. "Getting It Right: Protecting American Critical Infrastructure in Cyberspace." Harvard Journal of Law & Technology 20, no. 2 (2007): 403-22.

Crook, J. R. 2011. White House and Department of Defense Announce Strategies to Promote Cybersecurity, Including Strengthening Norms Affecting Internet Security. The American Journal of International Law, 105(4), 794.

Dingswerth, Kaus, and Philipp Pattberg 2006. "Global Governance as a Perspective on World Politics." Global Governance 12.

Fafinski, Stefan, William H. Dutton, and Helen Margetts. "Mapping and Measuring Cybercrime." Oxford Internet Institute, University of Oxford, 2010.

Finnemore, Martha and Sikkink, Kathryn. 1998. “International Norm Dynamics and Political Change,” *International Organization*, 52, 4, pp. 887-917

Glennon, M. J. 2012. State-level Cybersecurity. Policy Review, 171(Feburary/March).

Goldman, Jeff. “U.S., China to Cooperate on Cyber Security,” eSecurity Planet, May 8 2012, http://www.esecurityplanet.com/network-security/u.s.-china-to-cooperate-on-cyber-security.html

Goldsmith, Jack, and Tim Wu. 2006. Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford University Press.

Haas, Peter M., and Ernst B. Haas. 1999."Learning to Learn: Improving International Governance." Global Governance 1.

Hong Lu, Bin Liang, Taylor, Melanie. 2010. “A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States,” *Asian Criminology*, 5, pp. 123-135

International Telecommunication Union (ITU). 2005. “A Comparative Analysis of Cybersecurity Initiatives Worldwide,” http://www.itu.int/osg/spu/cybersecurity/docs/

Jaishankar, K. "Establishing a Theory of Cyber Crimes." International Journal of Cyber Criminology 1, no. 2 (2007).

_____. "Cyber Criminology: Evolving a Novel Discipline with a New Journal." International Journal of Cyber Criminology 1, no. 1 (2007).

_____."Space Transition Theory of Cyber Crimes." In Crimes of the Internet, edited by Frank Schmalleger and Michael Pittaro. Prentice Hall, 2008.

_____. "The Future of Cyber Criminology: Challenges and Opportunities." International Journal of Cyber Criminology 4, no. 1&2 (2010).

Jiang, Min. 2010. “Authoritarian Informationalism: China's Approach to Internet Sovereignty,” *SAIS Review* Vol.30, no. 2, pp. 71-89.

Joseph S. Nye, Jr. "Cyber Power." Belfer Center for Science and International Affairs, 2010.

Keohane, Robert O. "Multilateralism: An Agenda for Research." International Journal 45 (1990): 731-64.

Lessig, Lawrence. Code 2.0. Basic Books, 2006.

Liberthal, Kenneth and Singer, Peter. 2012. “Cybersecurity and U.S.-China Relations,” http://www.brookings.edu/~/media/Files/rc/papers/2012/0223_cybersecurity_china_us_lieberthal_singer/

Manson, G. P. 2011. Cyberwar: The United States and China Prepare for the Next Generation of Conflict. Comparative Strategy, 30.

Maurer, Tim. 2011. “Cyber Norm Emergence at the United Nations - An Analysis of the Activities at the UN Regarding Cyber-Security,” http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf

Milner, Helen. "International Theories of Cooperation among Nations." World Politics 44, no. 3 (1992): 466-96.

Park, Terrence. “Korean Cybersecurity Framework.” In 2009 ITU Regional Cybersecurity Forum for Asia-Pacific. Hyderabad, India, 2009. http://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/park-korean-cybersecurity-framework-sept-09.pdf

Peters, Anne, and Isabella Pagotto. "Soft Law as a New Mode of Governance: A Legal Perspective." In New Modes of Governance: NewGov, 2006.

Schafer, Joesph A. "Policing 2020: Exploring the Future of Crime, Communities, and Policing." Police Futurists International.

Segal, Adam. 2011. “China and Information vs. Cyber Security,” Council of Foreign Relations, http://blogs.cfr.org/asia/2011/09/15/china-and-information-vs-cybersecurity/

The White House. 2011. “The International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World,” http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Tikk-Ringas, Eneken. "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the Un First Committee 1998-2012." Geneva: ICT4Peace, 2012.

Wall, David S. Cybercrime: The Transformation of Crime in the Information Age. Crime and Society. Polity Press, 2007.

Wall, David S. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." Police Practice & Research: An International Journal 8, no. 2 (2011): 183-205.

Wu, Timothy. 1997. “Cyberspace Sovereignty? - The Internet and the International System,” *Harvard Journal of Law & Technology*, Vol.10, no. 3, pp. 647-66.

Wu, Timothy and Goldsmith, Jack. 2006. “Who Controls the Internet? Illusions of a Borderless World,” Oxford University Press.

ABSTRACT (KOREAN)

사이버안전(Cyber Security)과 국제협력: 중국과 미국의 입장 차이 분석을 중심으로

이 글은 오늘날 국제사회에서 중요한 문제로 부각되고 있는 사이버안전(Cyber Security)에 대한 중국과 미국의 입장 차이를 분석함으로써 향후 사이버위협 문제에 대한 국제협력 및 글로벌 거버넌스의 가능성과 그 형태를 전망하는 것을 목적으로 하고 있다. 본 주제가 갖는 중요성과 특수성을 설명하기 위해 먼저 사이버위협의 등장이 기존의 전통안보를 위한 국제협력과 어떤 면에서 다른지를 살펴본 후, 사이버안전을 위한 국제사회의 노력에 있어 반드시 고려해야 할 사이버공간의 위협이 갖는 특징들을 알아보고, 선행연구 및 유엔 공식문건 등 자료를 바탕으로 현재 국제무대에서 진행되고 있는 사이버안전 관련 담론의 흐름을 소개한다. 사이버공간의 등장으로 기존의 전쟁과 범죄, 테러행위 등 개념 간에 존재했던 경계선이 모호해지고, 국경을 실시간으로 넘나들 수 있다는 특성으로 인해 기존의 전통안보적 관점으로 접근하는 데에는 분명한 한계가 존재하기 때문에 이전과는 다른 접근법이 요구된다. 전통안보에서는 국가가 거의 유일한 참여주체였던 것과 달리 사이버위협에 대한 대응에 있어서는 국제협력 뿐

아니라 인터넷 서비스 사업자(ISP)와 같은 민간부문과의 긴밀한 협동이 필수적이기 때문에 이는 글로벌 거버넌스의 문제로 다루어야 한다는 것이다. 그러나 최근 일련의 담론들을 살펴보면 이제는 많은 국가들이 사이버안전을 국가안보(National Security)의 필수적인 부분으로 인식하고 있으며, 국경을 넘나드는 사이버범죄에 대응하기 위해서 각 정부의 협력이 필수적이라는 점을 감안하면 여전히 국가가 가장 영향력이 큰 중요한 주체라는 점을 알 수 있다. 또한 1998년부터 최근까지의 유엔 총회 제1위원회에서 각국 정부가 표명한 입장들을 살펴보면 앞으로 2012년부터 시작되는 제3차 정부전문가그룹(Group of Governmental Experts) 연구에서는 앞으로 국가주권과 같은 국제법적 개념이나 국제무력분쟁법을 어떻게 해석하고 적용할 것인지와 같이 국제법과 관련된 이슈가 본격적인 쟁점으로 떠오를 것으로 전망된다. 여러 국가 중에서도 이 쟁점, 즉 사이버공간상 국가주권 등 국제법적 쟁점에 대해 가장 큰 입장 차이를 보이고 있는 국가인 동시에 국제무대에서 가장 큰 영향력을 행사하는 국가는 바로 미국과 중국이며, 따라서 이 글에서는 유엔 공식자료와 양국의 정부공식 문서를 바탕으로 양국의 입장 차이를 분석한다. 이를 바탕으로 앞으로 사이버안전을 위한 국제협력에 있어서는 경성법(Hard Law)보다는 연성법(Soft Law)이 토대를 이룰 것으로 주장한다.