Master’s Thesis of International Studies

Information Security in the Cyber Era:
A Comparative Study on Cybersecurity Act Implemented in the United States and China

사이버 시대의 정보 보안:
미국과 중국의 사이버보안법 비교연구

August 2020

Graduate School of International Studies
Seoul National University
International Area Studies Major

Eunju Oh

Abstract

The past decade in cyberspace witnessed state-mediated attack in pursuance of accomplishing one’s political end. Once limited to opportunistic private criminal groups, the concept of cyberattack transformed into a country’s important means to bolster national security and further propagate national stance in cyberspace. Henceforth, cyberspace emerges as compelling security realm. When compared to traditional security environment, judging the situation is convoluted on account of the unique characteristics of cyberspace. Under the amorphous nature of cyberspace, if anything, nations become more nationalized. The nature of cyber realm characterized by innate openness and hyper-connectivity will trigger structural change in cybersecurity landscape. Thus the thesis argues that although nations will actively interact and engage in collective initiatives fueled by the rising voice of forming global governance for cybersecurity, the overriding state sovereignty in the end would breed discord in the cyber era. Every move in cyberspace rests upon a nation’s political end thereby taking account of geopolitical interests assumes greater importance since invisible borderline matters.

Given the nations’ inclination to utilize cyber capabilities for political ends, what happens in conventional security realm can also occur in cyberspace. The thesis chooses the US and China, allegedly Group of Two (G2), to study how both country take governmental measures vis-à-vis cybersecurity. Two great powers, with no doubt, are the pioneers in this emerging security realm. Not only both actively engage in building up cyber capabilities but also actively engage in appealing for cooperation to its allies. By conducting a comparative study on Cybersecurity Act of 2015 in the US and Cybersecurity Law of the PRC in 2016, the thesis aims to demonstrate how G2 implement legal regulation to safeguard domestic information infrastructure amidst the rising cyber threats posed by both state and non-state actors. In doing so, the thesis will research how respective country exerts its national interests in cyberspace while cooperate with other countries to defend global security. The thesis will add a new dimension on current cybersecurity studies by filling the gaps in previous literature. The thesis will contribute in understanding Sino-US relation regarding hegemonic competition in cyberspace and further propose the prospects of nations in the cyber era.

Keyword: Cyber Era, Cybersecurity Act of 2015, Cybersecurity Law of the PRC,
United States, China
Student Number: 2018-25679

Table of Contents

Glossary

APT: Advanced Persistent Threat

C2: Command and Control

CAC: Cyberspace Administration of China

CCP: Chinese Communist Party

CII: Critical Information Infrastructure

CISA: Cybersecurity & Infrastructure Security Agency

CISA: Cybersecurity Information Sharing Act

CNI: Critical National Infrastructure

CNII:China National Information Infrastructure

CNNIC: China Internet Network Information Center

CSL: Cybersecurity Law of the People’s Republic of China

CTTIC: Cyber Threat Intelligence Integration Center

DHS: Department of Homeland Security

DOC: Department of Commerce

DOD: Department of Defense

DOJ: Department of Justice

DOS: Department of State

DoS: Denial of Service

DOT: Department of Transportation

DNI: Director of National Intelligence

FBI: Federal Bureau of Investigation

FISMA: Federal Information Security Management Act of 2002

G2: Group of Two

HSPD: Homeland Security Presidential Directive

ICS: Industrial Control Systems

ICT: Information and Communications Technology

IGF: Internet Governance Forum

IoT: Internet of Things

IPS: Intrusion Prevention Systems

ISAO: Information Sharing & Analysis Center

MLPS: Multi-Level Protection Scheme

MPS: Ministry of Public Security

NCCIC: National Cybersecurity and Communications Integration Center

NCSC: Naval Command Support Center

NCTC: Naval Combat Training Center

NIST: National Institute for Standards and Technology

NSC: National Security Council

NSS: National Security Strategy

OIW: Offensive Information Warfare

OMB: Office of Management and Budget

PLA: People’s Liberation Army

PRC: People’s Republic of China

SCADA: Supervisory Control And Data Acquisition

SCO: Shanghai Cooperation Organization

STEM: Science, Technology, Engineering, and Mathematics

UNGGE: United Nations Group of Governmental Experts

Lists of Tables

Lists of Figures

I. Introduction

1. Research Background

Cyber era refers to the age when traditional sense of borderline becomes blurry and meaningless. With advanced technologies in cyberspace, the world is witnessing ceaselessly evolving cyber environment. Not only the advanced technology benefits all walks of life, it also transforms the spectrum of warfare, politics, economy, and military. Accordingly, the concept of cybersecurity comes to the fore front. When compared to traditional area of national security, cyber environment has a stark difference. Ostensibly, neither national borderline nor physical demarcation matter in cyberspace. Despite the unique characteristics of cyberspace, paradoxically nations become more nationalized. Once limited to opportunistic private cyber criminal groups for the sake of economic gains, cyberattack now is perpetrated under nation-level for the sake of one country's specific political ends. Thus the notion of cybersecurity goes beyond the concept of mere hacking which aimed at disturbing system or exploiting intelligence assets. That is to say, the concept of cyberattack has transformed into a country's important means to bolster national security and consolidate national interests. Current circle of influence encompasses IT industry, commerce, politics, military, international law, and thereby making future prospects of cybersecurity dynamic much more complex.[1] Cyberattack is no longer an instrument of private hackers or terrorists groups. In the name of national security, even a country regulates import and export of IT products internationally. The

[1] Kim, 2019

concept of cybersecurity is used to cement an alliance or even instigate arms race regarding advanced technology.

As aforementioned, the concept of nations in cyber era therefore deserves attention. Since the victims of cyberattacks encompass from individual or specific groups in a narrow sense to entire social infrastructure, experts encourage stakeholders including nations to form a shared responsibility to combat cyber risks. Regarding the debate on cyber age, the most controversial topic is how nations will protect themselves beneath allegedly invisible borderline. Although nations will actively engage in collective initiatives and forming global governance for cybersecurity, the overriding state sovereignty in the end will breed discord. In order to combat threats in cyberspace, there is and will be continuous collaborative efforts to prevent cyber victims. On closer scrutiny, however, the past decade showed state-led cyberattack which could possibly lead to physical damage. The advanced persistent threat (APT), in particular, posed by both state and non-state actors in the past decade have been demonstrated how these cyberattack could possibly lead to physical damage. 2013 Mandiant report, for example, accused People's Liberation Army (PLA) Unit 61398 for systematically stole data assets, intellectual property from over 140 US-based companies and major industries. The report attributes disclosed security breaches to APT strategy. Funded by the government, APT is allegedly the most persistent form of attack in China. The report concludes Chinese Unit 61398 corresponds to recently prevalent cyberattack towards US industries since the location of Unit 61398 is stationed in exact same location of disclosed APT activity.[2]

[2] Mandiant Report, 2013

International community is well aware of the impact of ever-advancing cyber technology given the latest nations' inclination to utilize cyber capabilities for political ends. Many expert express concern over assuming cyberspace as the fifth realm of national security followed by conventional areas exemplified by land, sea, air and space. Under this prediction, what happens in traditional security realm can also occur in cyberspace. For the reason above, the thesis aims to study this emerging security realm. The study chooses the US and China, so-called Group of Two (G2), to conduct a comparative study on legal regulation of information security inspired by domestic cybersecurity situation in respective country. In doing so, the thesis will demonstrate how respective country exerts its national interests in cyberspace. Moreover, the thesis will view how hegemonic competition forms between two rivalries in cyberspace.

2. Argument Overview

Along with the rising importance of 4th industrial revolution, 5G Technology and ICT advancement, the topic of cybersecurity is no way to be negligible since cyberattack inflicts damage on citizens, business, industries, and even national security. The physical borderline is not bound by the demarcation in cyberspace owing to the unique characteristics of cyberspace. The nature of networked cyberspace exemplified by innate openness and hyper-connectivity will trigger nations to interact in transnational sense. Recent propensity of cyberattack, however, turned out to be state-mediated attempts. This sparks the concept of nations in cyber era. In this sense, the thesis will argue the following. Nations will actively interact and engage in collective initiatives along with the rising voice of forming global governance for cybersecurity. Nonetheless, the overriding state sovereignty over shared interests upon cyberspace in the end will breed discord in the cyber era. Given a series of recent state-sponsored cyberattacks, it is convincing to purport that every offensive and/or defensive move rests upon a nation's political end. Since every move in cyberspace is under the guidance of the state, not just the target of an attack but also the following consequence reflects nation's security perception. Regarding supremacy of security in a traditional sense, the advanced countries possess key competitive advantage, whereas the opposite case is more likely in an unconventional security realm such as cyberspace. The reverse situation – the developing countries dominate advantageous position tantamount to that of the advanced countries – is feasible since the matter of information gathering preponderance over counterpart is unclear. In the cyber age, not the physical borderline but rather invisible borderline is important and it can create another tension.

The thesis chooses the United States (US) and China to make a comparative study on legal regulation, which is devised to protect domestic cybersecurity. Two great powers, with no doubt, are the pioneers in this emerging security realm. Not only both actively engage in building up cyber capabilities but also actively engage in appealing for cooperation to its allies. In case of the US, the country proclaimed allegedly war on cyberattack during Obama administration followed by the prolonged war on terror under two terms of Bush administration. China, at the same period, spurred the development of cyber capabilities under the leadership of Xi Jinping. By conducting a comparative study on Cybersecurity Act of 2015 in the US and Cybersecurity Law of the People's Republic of China (PRC) in 2016, the study aims to demonstrate how G2 implement legal statute to protect domestic information infrastructure and regulate operating system under the looming danger of cyberattack such as cyber terrorism and cyber espionage. Amidst the rising cyber threat posed by both state and non-state actors, the thesis will contribute in today's cybersecurity studies by filling the gaps of previous literature. The thesis adds a new dimension to understanding Sino-US relation, especially in regards to hegemonic competition in cyberspace. The study further aims to contribute in prospects of nations in the cyber era.

3. Significance of the topic

Threats to cyberspace have increased dramatically in the past decade. Under the rising importance of the 4th industrial revolution followed by 5G technology and ICT advancement, the notion of nation in cyber age come to the fore. The perception of global security threat transformed from traditional to non-traditional security threat including cybersecurity attacks. CSIS conducted an extensive research on cyber incidents targeting government agencies, defense industries, and technology enterprise. In total, there were 490 significant security breaches over the past decade with economic losses estimated to be about more than a million dollars.[3] Accordingly, the cybersecurity-related industry is booming. The cybersecurity market share is growing exponentially from $3.5 billion in 2004 to more than $120 billion in 2017.[4]

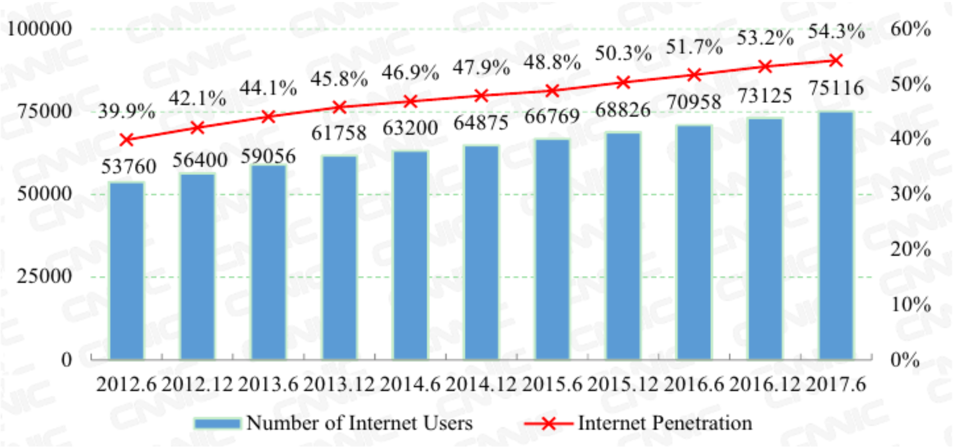
The Asia-Pacific, more than anywhere else in the world, is the most active region when it comes to cybersecurity. Asia-Pacific certainly made strides in terms of digital

[3] CSIS, 2020

[4] Ross, 2016

innovation by boosting the internet and allied industries. The more the industry flourishes, however, the more the region is exposed to cybersecurity vulnerability. The CISCO 2018 study reveals companies located in Asia-Pacific receive six threats every minute and yet only a half percent of total cyber aggressions are being investigated.[5] China, in particular, is a typical example of country with rapid growth as well as ceaseless cyberattack.

Figure 1. The size of internet users and internet penetration in China



Note. Adapted from CNNIC

As of June 2017, total internet users in China passed the 751 million. Within a half year, 19.92 million joined internet industry in China. The percentage of internet penetration increases as the number of internet user increases, and reportedly about 54.3% of internet users experienced the cyberattack. Among the internet users, 724 million are mobile internet users. Regarding the number of website, there are total 5.06 million websites as of June 2017. China ranked second in the world with reportedly 338 million of IPv4 addresses and 21,283 blocks/ 32 of IPv6 addresses.[6] Chins emerges as the most active

[5] Cisco Asia Pacific Security Capabilities Benchmark Study, 2018

[6] China Internet Network Information Center, 2017

country among Asia-Pacific in terms of investing cyber-related industries. China's meteoric rise in computer industry and willingness to utilize cyber capabilities for national purpose lends weight to the idea of nations become nationalized in cyber era. Among others, the US gives concern to China's aggressive action in cyberspace. The so-called hegemonic competition in cyberspace between the US and China became much more complex during Trump administration, which later sparked the Huawei scandal. Worrying voices are on the rise regarding the repercussion of the US-China trade dispute. The US was in the vanguard of boycotting Huawei. Bringing China's threat theory – also known as Chinese IT product conspiracy – to the forefront, the US refrained purchasing Chinese enterprises and products. The US also put pressure on its allies to boycott Huawei product and technologies. The US furthermore questioned links between Chinese government and big business. After all, the country banned Huawei network/products and prohibited transaction between ZTE and the US businesses up to seven years.

Given the points made above, keeping an eye on cybersecurity in today's complex environment deserves much attention than any other security realms for following reasons. First, it is the threat that affects directly to all levels of lives. It affects citizens, businesses, infrastructure and even national security. Second, threat types and mechanisms are still evolving, which means discerning the victims from perpetrators become blurry. Thus the study is significant in that this will give insights to current cybersecurity by focusing how respective countries act and interact to defend against looming cybersecurity threats. It will further discuss how G2 have applied divergent approach to protect domestic information infrastructure. The thesis will further contribute in understanding the future prospects of cybersecurity landscape.

4. Methodology

The thesis is qualitative study, comparative in structure. By conducting a comparative study on cybersecurity legal regulation implemented in the US and China, the thesis will analyze how the G2 lay the foundation for healthy cyber environment which is directly linked to national security of respective country. How the US and China protect domestic cybersecurity in the cyber era is the main research question of this thesis. The thesis also aims to tackle the following sub-questions. First, how the US and China define cybersecurity? What are the cybersecurity guidelines taken by two countries? Second, what progress has been made upon information security in respective country for the sake of building stable cybersecurity environment? Third, what kind of legislative step is taken in the US and China? Fourth, why the two countries advocate different legal approaches? And, by extension, what are the implications of future cybersecurity architecture?

The sequence of the study will begin by clarifying relevant concepts including cybersecurity, cybersecurity risks, cyber warfare, and cyber weapons. An overview of the Sino-US relation will be demonstrated along with previous literature on cybersecurity studies. To analyze cybersecurity legal regulation implemented in the US and China, each country’s basic guideline on cybersecurity will be described first. Cybersecurity strategy of respective country will be explored in order to verify on what grounds each country is endorsing their national stance. Then the study will examine Cybersecurity Act of 2015 in the US and Cybersecurity Law of the PRC in 2016. After analyzing two different roadmaps taken by the US and China respectively, the thesis will propose what these imply to future of nations in the cyber era given the ever-evolving cybersecurity dynamics. Lastly concluding thoughts, implications, and future challenges will be discussed. The research will refer to sources from relevant statutes, government report, security enterprises, major IT companies, and other online sources.

II. Literature Review

1. Sino-US relation and Cybersecurity

From a theoretical standpoint, the US-China competition springs from classical realism which argues that individual state in a state of anarchy seeks self-help by reinforcing national defense. The balance of power and security dilemma bring incremental investment in governmental measures including policymaking or drafting laws. Although the US gained supremacy followed by the end of Soviet-US confrontation, China made a meteoric rise – especially since early 2000s – comparable to that of US. Many assumed that China's rapid economic development would inevitably result in democratization, which is in a broader sense a part of Americanization.[7] China, however, unswervingly aims to recover the centrality of Asian geopolitics that the country enjoyed back in the old times. China is committed to their pre-established objective of solidifying Beijing's top position in Asia and phasing in a strict hierarchy which is respected by its neighbors. As a long-standing hegemon, the US clings to its stance of containing China.

In this situation, the phenomenon of balancing power is also witnessed in cyberspace. Fueled by the advancement of fourth industrial revolution characterized by 5G, AI, and Internet of Things (IoT), the idea of cyberspace becomes more salient. One obvious misperception, however, is viewing cyberspace as a global commons, which is wrong.[8] Each country with no doubt is exerting one's influence in cyberspace. When

[7] Tellis, 2014
[8] CSIS, 2010

examining the Sino-US relation with respect to cybersecurity, the disagreements between G2 over cyberspace cluster around five discussion items; first, the legitimacy of using cyberspace for a country's industrial and economic espionage; second, the legitimacy of exploiting cyberspace to enhance intelligence gathering; third, the feasibility of utilizing cyberspace for military operation; fourth, the rights of nation to regulate free flow of information within their borders; fifth, the matter of how international norms should be applied to individual country.[9] As if like security dilemma in a conventional sense, cyberspace is also witnessing security dilemma.[10] The ambiguous offence-defense differentiation in cyberspace in addition to negative perception toward counterpart's cyber capabilities will contribute in establishing cyber anarchy and ultimately will bring the US-China competition in cyberspace. On a closer view, mutual attack between the US and China is rampant especially in the past two decades. China's cyber-mediated attack towards the US information infrastructure leaves the country no choice but to consider confrontation and vice versa.

China's cyberattack on the US

Cyber spying on the US governmental branch: The US's grievance against Chinese cyberattacks cumulated in response to a series of cyber espionage through penetrations since the early 2000s. A few of cyber penetration led to grave consequences are cyberattacks targeting governmental and defense-related institutions including National Defense University, Naval War College, and Department of Energy laboratories.

F-35 fighter jet hacking incident: China's international reputation was damaged

[9] RAND Corporation, 2016

[10] Kim, 2015

after the US government revealed that China penetrated F-35 Lightening II program by Lockheed Martin and exploited data which is worthy of several terabytes[11].

Office of Production Management (OPM) hacking incident: Chinese government-sponsored hacktivist groups hacked into personnel information from the US federal agency in 2014.[12] The incident caused a big stir since allegedly hacked information even include fingerprint – under the fingerprint information, anyone can access to any of federal agencies.

Anthem Inc. hacking incident: The provider of health insurance in the US got hacked by outside perpetrator – allegedly based in China – and experienced personal data breach of total 80 million current and former members in January 2015.[13] Rich Barger, chief intelligence officer of ThreatConnect, remarked that malicious software discovered after the Anthem intrusion reportedly matches malware used to exploit FBI intelligence and US defense contractor.

Recently, Chinese government-sponsored hackers have expanded the target categories from trade secrets from corporations to a whole heap of personal data from government agencies that could be potentially used for purposes other than fraud or identity theft. Google, for example, accused China of extracting code repository through a server presumably originated in Taiwan en route for China, intensively during the period of December 2019 to January 2020. The researchers who discovered this intrusion

[11] Gorman et al, 2009

[12] Moon, 2018

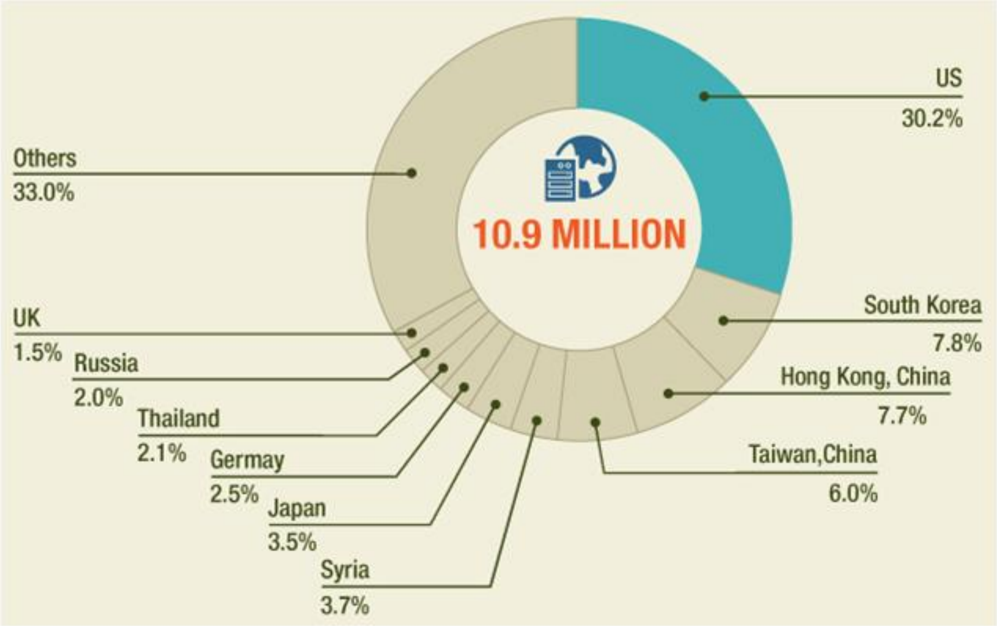
[13] Nakashima, 2015

named it Operation Aurora.[14] In addition, researchers working at McAfee discovered a series of attack and named it Operation Shady Rat. The server which was commonly found among external cyberattack housed hacked information of total 74 firms. The researchers accused China as a main culprit and named it Operation Shady Rat.

United States' cyber attack on China

Unlike that style of public accusation by the US against China, China relatively gives evasive answers to America's cyberattack. The official Chinese authority has been expressed its formal position that the US is the most active and frequent perpetrator in cyberspace targeting China's cybersecurity.

Figure 2. Reported cyberattacks toward China



Note. Adapted from China Daily

[14] Libicki et al, 2016.

China publicly accused the US by arguing that the US continues to take first place of controlling Chinese network servers. China argues approximately 10.9 million Chinese hosts were exposed and further manipulated by overseas servers in 2013.[15] Among this number, China revealed that 30.2 percent are based on the US.

Cyberattack on a national level is a weighty question. Cyberattacks intended to data manipulation could impair decision-making system among corporate executive and government officials since all of stored and/or received information asset is no longer reliable. In that sense, Sino-US conflict in cyberspace is a salient security issue. Nonetheless, both countries actually have tried to work together to tackle the topic of cybersecurity bilaterally.

US-China cybersecurity cooperation

The US showed belligerent attitude to China and vice versa during the first decade of 21st century. The matter of cybersecurity was discussed intensively during Obama administration and thus a number of summit talks regarding cybersecurity happened since 2008. It was only in 2013 when the US and China brought up cybersecurity as an important agenda. Accordingly, the US-China Cyber Working Group was launched at June 2013 summit and both discussed cybersecurity as a shared agenda at the US-China Strategic and Economic Dialogue. After a consecutive meeting since 2013, however, both countries agreed upon the necessity of mutual cooperation and importance of amicable relation. Finally, both reached an agreement on cybersecurity at the US-China Summit in September 2015. Amongst other cybersecurity threats, the

[15] China Daily, 2014

agreement narrowly focused on regulating cyber spying for commercial purposes. The US-China Cyber Security Agreement in 2015 is significant in the sense that, despite hostile climate in the past, it was a new effort to develop code of conduct to defend their common interests.[16] Taking the agreement at the face value, however, is impossible owing to mutual distrust and inherent vulnerabilities of both countries' cyber capabilities.

As abovementioned, what happened in traditional security realm could occur in cyberspace with a strong chance. What the US has been upholding for more than a century is rule of law in addition to free and open market with its allies. On the other hand, China's longing for development since the allegedly "Century of Humiliation" is noticeable in terms of modernizing military expansion, promoting domestic revolution, and ensuring a stronger presence in international stage. Modern power struggle aspect is way too complex than that of previous struggle between the US and Soviet Communism. The hegemonic competition in technological strength will determine future prospect of cybersecurity. To preserve US hegemony and its national interests, the country needs to formulate strategy vis-à-vis China. Unless multilateral efforts to prevent cyber anarchy continue, countries have to bear the security dilemma in cyberspace and the competition between the US and China will be continued. The best option now is balancing Beijing's growing capabilities by increasing China's stake in global order on one hand while raising the burden when abusing its power on the other.[17]

[16] Cho, 2017

[17] Ford, 2014

2. Previous studies on cybersecurity

The concept of cybersecurity in essence is applied differently from that of traditional security concept of the tri-service – land, sea and air – since the dividing line which distinguishes the attacker from the victim becomes blurry in cyberspace. The scope of damage varies from individual to a group of countries. For the most part, the meaning of cybersecurity is intermingled with other relevant terms and still lots of previous studies defy its correct definition. The concept of cybersecurity in the past was mainly dealt among computer scientists and information security specialists while the topic now is being addressed by policymakers as one of the major national security threats. Before delving into cybersecurity studies, clarifying relevant lexicons is needed.

Cyberspace, according to Nye (2011), is a man-made complex environment. Specifically, cyberspace possesses a physical infrastructure element including rival resources and sovereign jurisdiction in both economic and political sense. Nye argues that given the nature of cyberspace, if anything, one country's high dependence upon cyber systems to facilitate military and economic sector will create more vulnerabilities that can be attacked by both state and non-state actors.[18] In the same vein, Fisher (2005) argues cyberspace is a combination of information assets, physical components, and virtual structure. That is to say, it is composed of information that contains and physical components that mediate the flow of information under the virtually structuralized backdrop. Thus cyberspace comprises not just internet that is connected to computer, but also tons of electronic devices and systems that either directly or indirectly connect the

[18] Nye, 2011

whole system by devised mechanism. Even a computer without internet connection belongs to parts of cyberspace if it has a channel of communication with other computers through removable means.[19]

Kello (2013) suggests five difficulties when applying traditional concept of warfare in cyberspace.[20] First, the concept of so-called proximate cause of injury is missing in cyberspace because the injury per se could be non-violent. Second, the standard of offensive action in cyberspace does not meet the physical standard of using kinetic force such as duration, intensity, and the scope of influence. Third, innumerable cases of cyberattack are made by non-state actors who are not typically belong to the influence of international law thereby exposing lots of loopholes to those cyberattack perpetrators. Fourth, an offensive cyber operation has no strategic goals – just as in traditional warfare – if launched by non-state actors. Fifth, it is hard to cognize civilians from military targets when delivering a cyberattack due to the unique nature of network systems represented as interdependencies and broad diffusion.

The concept of cybersecurity refers to three-pronged acts or state of being. According to Fisher (2016), the first refers to a set of measures to protect computer networks, hardware or software device, or broadly speaking, information from outside disruption and/or attacks. Second, it refers to the state of being safeguarded from abovementioned threats. Third, the concept also encompasses extensive effort aimed at strengthening those activities.[21] Sims (2011) clarifies three goals as to why perpetrators

[19] Fisher, 2005
[20] Kello, 2013
[21] Fisher, 2016

in cyberspace make a malicious attack. First, attackers aim to damage or destroy the critical information infrastructure. Second, attackers try to gain unauthorized access to target's information system. Third, attackers attempt unauthorized access for the sake of information exploitation.[22]

Regarding the conceptualization of cyberattack, defining the extent and category of attack differs among experts. Geers (2008) describes five common tactics used in cyber warfare.[23] First is data modification. To conduct a successful data modification, a legitimate user has to conduct operation based on maliciously altered data. Second, propaganda is very easy and cheap tactic, often described as one of the most effective cyberattack operation. Third, espionage is conducted for the benefit of intelligence-gathering and can be completed from a far distance. Fourth, denial-of-service (DoS) is the most common strategy to create confusion so that the target is unable to respond to real requests for certain service. DoS tactics encompass from electromagnetic interference via voltage surges to physical destruction of hardware. Such DoS attack ultimately aims at website defacement or database attacks for destroying weapons or rendering Command and Control (C2) system useless. Fifth is infrastructure manipulation. The system of national infrastructure is vulnerable on two accounts. It is immensely connected to the internet and in most cases critical infrastructures are in the hands of private enterprises. The supervision of electricity, for example, is directly linked to national interests since electricity has no substitution and the rest of infrastructure rely

[22] Sims, 2011
[23] Geers, 2017

on it. Following three incidents are typical examples which applied frequently used cyberattack tactics.

Chechnya 1994: pro-Chechen forces and pro-Russia forces waged an internet war – or virtual war – in company with their conflict ground warfare. The Chechen separatist movement was considered as a pioneering action in terms of using propaganda tactics on the internet. Repulsive images such as bloody corpses were uploaded on internet to turn public opinion in opposition to Russian military excesses. When Kremlin officials denied the Chechen bus accident in 1999, images of accident immediately appeared on the web.[24] By means of developed IT, pro-Chechen forces enable streaming videos of their military activity thereby fulfilling their mission.[25]

Kosovo 1999: the early military engagement of NATO happened in 1990s followed by the tremendous growth of the Web and Kosovo in 1999 was its first large scale internet war. When NATO planes bombed Serbia, a number of Serbian hacker groups such as Blank Hand carried out an attack on internet infrastructure of NATO for the purpose of disrupting their military operations. Operating systems of NATO and US were attacked during the war using DoS tactics along with virus-infected emails. In total of 25 strains of virus were discovered later on.[26] The Serbian hacker groups allegedly argued that they paralyzed one of US Navy computer systems. NATO's public affairs website was virtually disabled for several days during the war and, since then, the organization began to update all of its networks and computer servers.

[24] Paul. 1999

[25] Foreign Military Studies Office, 2002

[26] Mi2g. 1999

Middle East 2000: immediately after the abduction case of three Israeli soldiers, the Hezbollah website was hacked. Pro-Palestinian hacker groups retaliated against Israel by attacking social infrastructure including political, military, media, and universities. Pro-Palestinian hacker groups launched an attack, in particular, targeting the economy. Unlike other web-mediated conflict, cyber war in Middle East demonstrated that political conflicts in internet era can easily become internationalized. The American Israel Public Affairs Committee (AIPAC), pro-Israel lobby based in the US, was hacked and experienced tons of economic loss owing to hacked emails despite the accusation that AT&T provided technical assistance to the Israeli government.[27]

Successful cyberattack encompasses detecting target's vulnerability, exploiting that vulnerability and subsequently executing a payload.[28] In many cases, cyberattack can demonstrate its real worth when supporting a country's military operation since the attack not only dispute counterpart's C2 system, but undermine adversary's combat capabilities by jamming the defense industrial base. Although cyberattack carried out for either offensive or defensive purposes can have tactical effects and strategic implications, but its indirect consequences far surpass than that of direct consequences. Today's information technology enables adversaries to readily initiate anonymous cyberattack. If a far more sophisticated authentication system is developed, nevertheless there still is a chance of network system improperly used by a third party.

Unlike the conventional weaponry used in traditional physical warfare, weapons in cyber domain are in the form of computer codes such as all sorts of malware that is

[27] TechWeb News, 2000

[28] National Research Council, 2009

devised to inflict harm. Given this, it is much more difficult for states to detect and picture counterpart's capabilities compared to the past when it was physically visible and easily detectable. Furthermore the nature of anonymity in cyberspace contributes to the notion of uncertainty. Building up cyber technologies, specifically security capabilities in cyber age, is much cheaper than equipping conventional weapons. Thus not only developed countries, but relatively weak countries can possibly participate into the cyber arms race and compete with other powerful states. By applying conventional arms race theory, Craig and Valeriano (2016) tried to conceptualize arms race in cyberspace. Mutually competitive military build-up and abnormal investment in weaponizing capabilities are the two variables to verify the actual armament race in cyberspace. Findings show that state dyads have been engaged in arms race in cyberspace especially in the past decade.[29]

Theoretically, cyber war employs systematic information processing – bytes, message, and malware – and by doing so attacks information system or information asset. In case of the US, cyber weapons will operate by making counterparts doubt on their system management to handle advanced technology equivalent to that of the US or US allies. Walt (2010) categories following four set of issues help framing the concept of cyber warfare. First, emasculate counterpart's military capabilities. Second, penetrate network in an attempt to jam the social infrastructure. Third issue is web-based cyber crime. Fourth is cyber espionage.[30] Unlike conventional warfare, warfare in cyberspace has a distinct advantage. Malignant code or virus, allegedly cyber weapons, does not

[29] Craig et al, 2016

[30] Foreign Policy, 2020

produce loss of lives and it is much cheaper to produce. Thus many countries including the US and China have an eye on developing relevant capabilities. The following three cyber incidents are categorized as cyber warfare by experts.

Estonia 2007: amidst the conflict between Estonia and Russia, the Estonian government moved Soviet memorial out of its capital in April 26, 2007, which aroused anger among Russian public and Russian minority inside Estonia. Starting from April 27, Estonia experienced three weeks of severe cyberattacks targeting its internet infrastructure and online banking system. Multiple DoS attacks crashed websites of Estonia's two largest banks. Given that over 98% of banking transactions is conducted through online, it was indeed a dire consequence.

Georgia 2008: Amidst conflict between Russia and Georgia over South Ossetia, Russia launched DoS attack against Georgian governmental website in company with their military bombardment. Central government website, Ministry of Defense, and Ministry of Foreign Affairs website were hijacked. Regarding Russia's DoS attack, Obama administration demanded Moscow to halt the cyberattack as well as asked ceasefire on the ground. The Russian Business Network (RBN), with the aid of Russian government and mafia, was accused of cyberattacks by computer analysts.[31] Followed by the barrage against Estonian governmental website in 2007, Georgian official websites are being bombard through DoS attack.

[31] The Telegraph, 2008

Iran 2010: The Stuxnet worm attack targeted industrial control systems (ICS). In this case, Iranian nuclear power plant's Programmable Logic Controllers was damaged.[32] As a result, the Natanz plant had to remove the virus and also replace all of equipments, resulting two year delay to the power plant's operating capabilities.[33] The attack paralyzed approximately 1000 centrifugals. Expected fraction of damage surpasses that of atomic bomb blast on Hiroshima in 1945. Unlike previous cyberattack, Stuxnet demonstrated that it can deliberately launch an attack against intended target and can inflict physical damage as well. Average cyberattack was in the form of data manipulation or data exploitation.

What is even scarier is that unlike the times of nuclear arms race during Cold War, anyone – including hacktivists, criminal organizations, rouge states, or terrorists – could easily obtain cyber weapons.[34] Lynn (2011) argues that cyber warfare with no doubt is imminent threat to the US. Lynn introduced five pillars of cyber defensive strategy. First, identify cyberspace with conventional operational domain such as land, sea, and air. Second, implement active defenses to ward off malicious code or software attacks. Third, invest in securing commercial networks that run critical infrastructure of a country. Fourth, cooperate with allies for collective cyber defense system. Fifth, prioritize mobilizing industry with redesigned network technology.[35]

Denning (2013) defines active and defense strategy in cyberspace. Active cyber defense refers to a defensive action in order to destroy or nullify the target's effectiveness

[32] Schneier, 2010
[33] Jerusalem Post, 2010
[34] Park, 2011
[35] Foreign Affairs, 2011

and operability against one's assets and friendly forces while passive cyber defense refers to all measures taken to minimize effectiveness of target's cyber capability. Currently many security control agencies employ active cyber defensive measures. Active cyber defenses include access controls (preventing unauthorized access to files and resources), user authentication mechanism (block adversaries' login attempts), intrusion prevention systems (IPSs), anti-malware systems, and firewalls (identify malicious software and block anomalous behavior). Passive cyber defensive actions range from verification, cryptography, configuration monitoring, steganography to vulnerability assessment. It also includes all actions regarding risk assessment, recovery and backup of lost data, and training of users. Denning argues that active cyber defensive measures should be employed and connected only when authorities grant an action through appropriate contracts, policies, law. Given this, government – in addition to law enforcement body, defense arms, or related security agencies – have much more power and validity rather than the private sectors in terms of exercising non-cooperative active cyber defenses.[36]

Meanwhile, Libicki (2011) invokes the FUD (fear, uncertainty, and doubt) conception.[37] The uncertainty-and-doubt strategy works in following sequence. First, a target agent recognizes that its system or equipment has been hacked. It will estimate outcomes of virtual war and the agent will decide whether to go to war. Given the characteristic of cyberspace, a preemptive attack is likely to have significant advantage, especially if the attack is in the form of strategic surprise. In order for cyber weapons to wield strong influence, its wheel of influence should encompass to the population at large.

[36] Denning, 2014
[37] Libicki, 2011

Added to this, pre-designed cyberweapon has to be frightening in that the perpetrators can derive benefit from the target's reaction or concession. As far as information systems is concerned, high wining rate is in the hands of a country with traditional superiority than that of third-world countries. Libicki points out that third-world countries' incompetent capacity to produce cyber capabilities including cyberweapons and cyber warriors may be attributed to less-developed educational facilities and poor recruitment base. Those who can't afford to play at that level will hesitate in entering the battlefield at the outset. Developing offensive cyber capabilities to inhibit rouge states or others who aim to contest the US' military strength from investing in the same field is such case.

3. Cybersecurity and relevant legal regulation

a. The United States

Lynn (2010) argues although US benefits from its advanced digital infrastructure more than any other nations, the high dependency among operating network system is vulnerable and ultimately enables other adversaries to exploit intelligence which potentially could disrupt the nation's economy. The low price of computing devices also lowers the entry barriers for US adversaries to deliver cyberattack since perpetrators do not have to invest in building costly weapons such as aircraft carriers or stealth fighters to pose a threat to US national interests. In this regard, the US government's capacity to defend its cyber network lags behind that of adversaries' capacity to exploit the US cyber vulnerabilities. The US must consistently develop and improve its defense capability to precede other pursuers. The target for a cyberattack is not just US military, but social infrastructures including transportation networks, financial systems, and power grids. Nonetheless, the US still has unparalleled technological prowess and the country can utilize this into superior military strength in cyber domain. Lynn argues that current US defensive measures should be transformed proactively. According to Lynn, active defense is possible if the Defense Department put its cyber defense capabilities under one roof to efficiently detect any attack attempts or intrusions.[38]

Clark and Levin (2009) criticized that nation's information asset is precariously exposed to cyber risks since the country's information infrastructure is highly dependent on internet-based. The government believes merely obliterating traces of cyber sabotage, data theft, or electronic infiltration is neither technically feasible nor cost-effective measures. What government can do at best is concentrate in investing in sensible risk management. Washington should adopt integrated control system that addresses previous sprawling communications network. Experts assume that US is already engaged in low-intensity cyber warfare represented by information theft. From private intrusions to systematic attacks, the country is witnessing increased frequency of network-based attacks. Current status of the country's infrastructures ran by few hardware operating systems, after all, leaves the country's digital infrastructure predisposed to external infiltration and threats. In this regard, Clark and Levin recommend the US focus on diversifying and reshuffling the country's digital infrastructure.[39]

In case of US, although the jurisdiction over cyberspace is transferred to executive office of the presidency, there is still a lot to consider. Harknett and Stever

[38] Lynn, 2010

[39] Clark et al, 2009

(2009) suggest allegedly cybersecurity triad which is consisted of three layers when viewing current status of the US cybersecurity. First pillar is intergovernmental relationship, which is defined as relationship between federal and local governments. Second pillar is public-private cyber relationship – i.e. government to private sectors, and especially private enterprises that run critical infrastructure. Third pillar is integrating the relationship in between general population. Among three mentioned triad, public-private cyber relationship is challenging in that both parties have unaligned priorities added to the generally agreed sentiment that cyber vulnerabilities is an acute problem. Thus, the basis should be focused on better coordination rather than better centralization when seeking solution to cyber vulnerabilities. The impact of computer technology to civilian population is considerable and thus full societal engagement is required when taking measures in protecting cyberspace. In this regard, federal government's innovative plan will be no avail unless intergovernmental policy dimensions with overall agreed threat perception are considered.[40]

Park (2017) pinpoints social and political consensus was already taken place in the US for the purpose of establish legal framework to secure cyberspace. Park argues that the CISA, enacted in December 2015, is a gist of Cybersecurity Act. CISA establishes guideline for privacy and civil liberties. Private subjects can monitor their registered information system in an attempt to verify security in cyberspace and they also can monitor others' information system when authorized by law. According to CISA, those who submit their contents of information can discharge any liability. Cybersecurity

[40] Harknett and Stever, 2009

Act overtly emphasizes that the Act per se does not impose any sorts of duty to share information mandatorily, but rather encourages private subjects to join information sharing by providing proper legal immunity. The Act focuses on damage prevention of information breach from external cyberattack or cyber espionage. Park also distinguishes the role between DNI and DHS. While the DNI is responsible for establishing procedures for sharing, the DHS is responsible for establishing procedures when receiving information on behalf of the government. Based on the voluntary principle, the Act aims to form secure information community under the guidance of DNI.[41]

Cybersecurity is regarded as one of the most imminent security problems in the US and the governmental efforts including preparing a relevant legal provision and policy to combat cybersecurity threats have a long history. The naysayers criticize Cybersecurity Act by saying that the law commits invasion of privacy of excessive number of citizens. The Act focuses on multi-level cooperation among private enterprises, local government, state government and federal government.

Ahn (2018) addresses how the discussion on cybersecurity act has been evolved and how the law is implemented two years after the implementation. The cybersecurity legal provision in the US attempts to narrowly deal with the protection of information infrastructure which governs the entire society. Most of the US infrastructure, in fact, is operated by private enterprises and it is challenging for those operators to pursue profit-making while at the same time serving the duty of providing universal service to the public at affordable price. Current legal provisions focused on preventive measures rather

[41] Park, 2017

than follow-up measures. Many also concern regarding balancing between protecting personal information and safeguarding information security in broader sense.[42]

b. China

China's course of action in a broader sense is similar to other Western countries in a way that the country aims to protect homeland network and information system against external cyberattack or cyber crime. Given the country's sociopolitical feature, however, China takes different route, especially when it comes to cybersecurity strategy and relevant legal provisions. Lim (2017) argues five characteristics in China's cybersecurity strategy. First, the gist of the security strategy is strict control along with regulation upon information circulation system. Second, the country attempts to elevate cyber threat to a higher national security threat. Third, the security regime in cyberspace states that it will pursue securitization of cyberspace and informatization at the same time. Fourth, establishing comprehensive cyber decision-making body and enhance domestic monitoring capacity. Fifth, the country will contribute in forming international consensus on cybersecurity standard. It is undeniable that China, as a communist country, has been pursuing top-down decision making approach. When it comes to drawing up cybersecurity strategy, however, the country is willing to embrace outside opinions by opening hearing session biennially and allow gathering the policy recommendations from hands-on workers and expert groups.[43]

[42] Ahn, 2018

[43] Lim, 2017

Compared to other countries' national stance on cybersecurity, China advocates quite different ideological route. Kim (2017) argues principle of non-intervention and the concept of cyber sovereignty are two most important keynote of China's cybersecurity strategy. Based on abovementioned cyber doctrine, China aims to equip cyber capabilities comparable to that of the US. Ever since the allegedly Snowden disclosure in 2013, in particular, China spurred the development of cyber capabilities and is forming hegemonic competition with the US in cyber domain. China's ultimate goal is to get ahead of US in terms of cyber capabilities and build global internet governance while China stands in the vanguard. In the beginning, China's cybersecurity strategy revolves around protecting domestic information infrastructure against external cyber threat while at the same time defending its sovereignty in cyberspace from outsiders' intervention. Since Xi took office, however, the country's cybersecurity strategy displayed a tendency to adopt more offensive measures. Materializing national defense objectives and installing special military units show China's attempt to adopt more offensive strategy. In regards to international cooperation, China is appealing to region based international organizations and other like-minded countries, especially those in developing countries including African countries, to form a new unified front against that of the US.[44]

Seo (2017) indicates that China began to pay attention to enacting a law regarding personal information protection on account of the rising voice of privacy infringement. As the economy grew exponentially, the commercial value of personal information is appreciated in value. At the same time, the development of ICT brings the

[44] Kim, 2017

danger of infringement of personal data and triggers cyberspace far more vulnerable to cyberattacks. E-commerce, in particular, is flourishing inside China thereby gathering, protecting, and controlling personal data asset is far more important than ever. Thus building a credit society is one of the country's main goals since the inauguration of Xi Jinping. Formulating a comprehensive protection system for individual and private sectors is needed. The Cybersecurity Law of PRC is an archetype after years of the authority's hard work. The law adheres to its firm goals including network security management, personal information protection, to uphold national interests and values. Although the country receives harsh response from foreign companies inside and out, but the future looks like it will maintain current legal binding force otherwise adding more regulating provisions.[45]

Cho and Cheong (2016) contend the growing concerns inside over evolving cybersecurity landscape owing to the inherent nature of internet represented by openness and interconnectivity. Added to this, the authors point out that high dependence of Chinese technology upon foreign countries is another crucial factor why China is eager to achieve technology independence. China assumes investing enormous amount of budget on cybersecurity will directly bolster national security and interests. In this regard, China drafted legislation for the purpose of combating internet hacking, safeguarding digital information and relevant cyber technologies. Furthermore, China criticizes the current cybersecurity architecture by arguing that western power, especially the US, already is holding dominant position. Other countries including China face danger due to

[45] Seo, 2017

this unbalanced cyber environment. China purports that developing countries – so-called second mover – should, in this context, all cooperate in the midst of ever-changing cybersecurity environment.[46]

4. Limitations of prior research

Previous literature comprehensively studied on cybersecurity in relation to international relations, focusing on conceptualizing this relatively new security realm. Scholars have studies a series of cybersecurity-related lexicons in-detail. Concerning the case study of US and China, prior research well annunciates the danger of current status of cybersecurity the in respective country. Nonetheless, there are few limitations of prior research. First, previous studies scarcely touched upon viewing cybersecurity in relation to geopolitical perspective. Given the recent decade of state-mediated cyberattack, understanding country's political act in cyberspace and examining cybersecurity landscape in terms of traditional geopolitical interest also is required. Second, prior research focused on describing cybersecurity strategy in a narrow sense. Most of prior research only viewed cybersecurity which directly affects one's national security. Thus, in terms of implementing cyber regulation, literature narrowly focused on either explaining the cybersecurity strategy or reprimanding country's mass surveillance activities – in the name of national security – while actually enforcing the legal regulation. Lastly, there is no direct comparative study on cybersecurity act implemented in the US and China. This study adds a dimension to current cybersecurity studies by focusing on the underlying reason for implementing cybersecurity legal regulation in

[46] Cho and Cheong, 2016

both countries. In order to demonstrate the concept of nations in the cyber era, the selected two pioneering countries' discussion over cybersecurity, the keynote of relevant legal regulation, underlying reasons for adopting regulatory approach respectively, and further implications will be studied.

III. The United States

1. An overview of national security and cyberspace

a. Cybersecurity environment

The most vexing challenges the US will face is those of transnational security threats including climate change, cyber theft, epidemic diseases, transnational crime, and human trafficking. Among mentioned challenges that transcend national borders, the US especially place importance on security threat in cyberspace. Threats in cyberspace have been increased and evolved exponentially in the past decade. Keeping an eye on cybersecurity deserves much attention than any other security realms. Every country ends up with different solution to cybersecurity risks owing to respective country's security environment, threat perception, and international status. The deeper the internet connection, the harsher the consequence will be. Although the US currently enjoys one of the most advanced technology and manpower, many scholars have addressed the possibility of network operating system being abused by external perpetrators, which is consequential to national security. The worst scenario is critical national infrastructure (CNI) of the US being damaged by terrorist organizations or other extremists through conducting offensive information warfare (OIW).[47] Mounting concern over data privacy also bolsters the importance of securing data against malicious OIW operations.

Under the cybersecurity environment endangered by prevalence of sophisticated cyberattacks, current state of America's cybersecurity environment in both public and private sector is not only vulnerable but also defenseless. Supervisory Control And Data

[47] Valeri, 2000

Acquisition (SCADA), the industrial control system to operate primary power plants and other public utilities, are closely connected to the Internet.[48] Cyber perpetrators could abuse internet connectivity to disrupt or further damage operating system. Private sectors, in particular, have been witnessed a series of acute problems. Westinghouse Electric Co., JPMorgan, and Target – each represents one of the influential enterprises in nuclear, financial, and retail industry– are hacked by outsider.[49]

Cyberattack on network system operating Critical Information Infrastructure (CII) is fatal to society and national security. Two most common cyber threats to America's CII are cyber espionage and cyber terrorism. Foreign espionage, especially in terms of industrial and economic espionage, poses significant threat to nation's security and prosperity.[50] Leon Panetta, former US Defense Secretary, stressed the grave importance of cyber terrorism. Panetta made a remark that the extent of damage by a violent extremist group's cyberattack can excel that of destructive September 11 terrorist attack.[51] This could possibly jeopardize whole American information infrastructure. Using malicious software called WannaCry, for example, social infrastructures in certain countries have been hacked in 2017. The range of victim group includes FedEx, Britain's National Health Service, and Russian Interior Ministry. Unlike typical ransomware attacks which encrypt small and medium sized files using malicious program, WannaCry attracted worldwide attention since victims include vital organizations and institutions that comprise CII system.

[48] National Communications System, 2004
[49] Eastman, 2017
[50] NCSC, 2018
[51] Garamone, 2012

As a matter of fact, 85 percent of the country's CII is run by the private sector.[52] Given the structure and peculiarity of American cybersecurity environment, any kind of cyberattack towards information infrastructure will bring much more deadly consequence. Added to this, the wears and tears of infrastructure in the US is a matter of cardinal importance.[53] Network operating system of American CII being outdated and in need of comprehensive update also demonstrate loopholes of the present state of cybersecurity environment in the US. The number of dams rated as deficit, for example, has tripled from 1999 to 2008 and this aging tendency is the prime reason to potential failure.[54] Given that the majority of the infrastructure is owned and managed by private entities, financing maintain facilities and protecting against external cyber threat are not a straightforward issue. Those private entities running CII systems are responsible for protecting their own system, but in fact it is hard for private entities to allocate resources under the tight budget because they are not commercial entity in essence. Owing to private sector's high dependence upon IT systems, vulnerabilities are inherent.[55] Currently four parties – Congress, government agencies, law enforcement agencies, and the military – share the burden of cybersecurity and tackle the matter of CII protection altogether against external cyberspace-mediated threats. A thorough review on cybersecurity environment and relevant monitoring mechanisms are needed to bolster the country's cybersecurity defenses.[56]

[52] Government Accountability Office, 2009
[53] Federal Emergency Management Agency, 2011.
[54] Dalton, 2008
[55] Rodin, 2015
[56] Chung, 2018

b. Cybersecurity strategy guideline

"Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation" – NSS (2010)[57]

When placing responsibility on each federal office, the cybersecurity implementation system introduces three-layered system to seek policy integration and cooperation among relevant federal offices. Under Bush administration, both Department of Homeland Security (DHS) and Department of National Intelligence (DNI) take the overall responsibility. During first term of Obama administration, Cybersecurity Directorate under the National Security Council (NSC) gives direction to relevant federal offices. Working-level federal offices such as DHS, DNI, Federal Bureau of Investigation (FBI), Department of State (DOS), and Department of Commerce (DOC) carry out its own mission individually. During Obama's second term, three agencies – Cyber Threat Intelligence Integration Center (CTIIC), E-government cyber unit, and lastly Information Sharing & Analysis Center (ISAOs) – are added to enhance public-private partnership. CTIIC detects cyber threats along with potential risks to provide preventative information to relevant organizations. E-government cyber unit under the Office of Management and Budget (OMB) assists federal offices' mission. The National Cybersecurity and Communications Integration Center (NCCIC) is installed under the DHS to promote effective information sharing between public-private entities.

The long-standing national security goal of the US is renewal of American leadership in the 21st century. In regard to bolster homeland cybersecurity situation, NSS

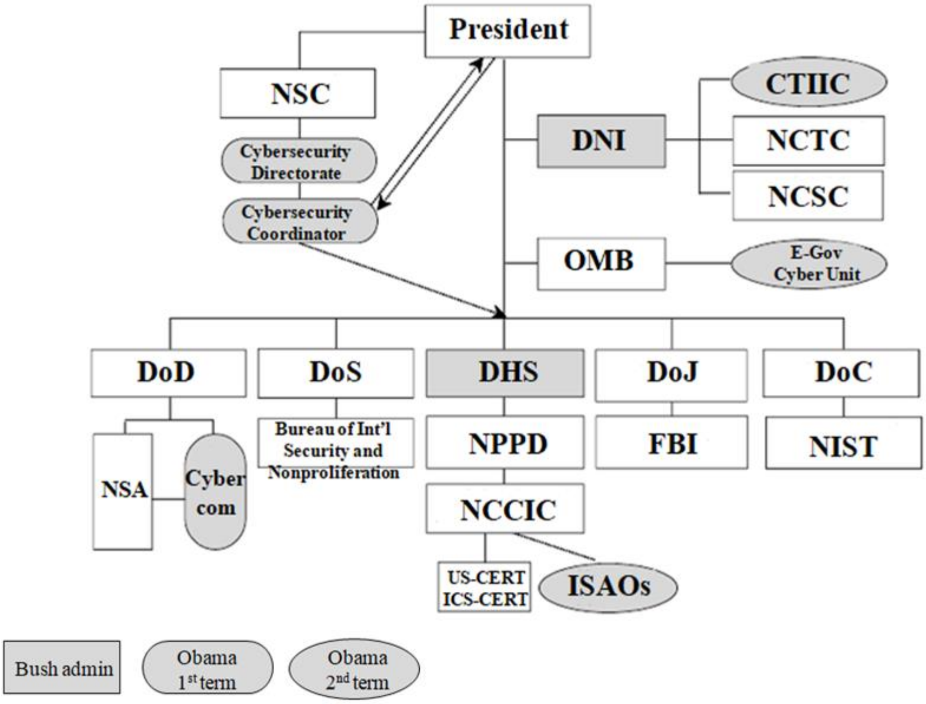
[57] National Security Strategy, 2010

2010 publicly clarifies security goal of protecting digital infrastructure as national strategic assets. It also emphasizes safeguarding civil liberties and privacy at the same time. In case of cybersecurity, the country pronounces conducting a comprehensive national campaign to build a stable digital workforce and promote cybersecurity awareness. Under the belief that future of America's leadership depends on coming generation, the Obama administration promised to commit in educating future innovators and scientists by investing vastly in so-called STEM (science, technology, engineering, and math education).[58] The country internally adopts two strategies, which are securitization and militarization.[59] In terms of alliance strategy, the US appeals to its like-minded allies for cybersecurity cooperation.

In line with the Bush administration's keynote, Obama administration published Comprehensive National Cybersecurity Initiative (CNCI) in 2009. The Initiative elaborated main objectives in defending homeland cybersecurity. Specified fundamental objectives encompass protecting communication networks, information infrastructures, civil liberties, and privacy rights.[60] The Initiative emphasizes that specified objectives could not be achieved unless strengthening capabilities of primary government agencies proceed in advance. The US assigns the responsibilities and tasks to corresponded federal agencies in order to safeguard homeland cybersecurity and to advance national interests in following order.

[58] The White House, 2010
[59] Sheen, 2016
[60] The White House, 2009

Figure 3. Organizational chart of the US cybersecurity



Note. Adapted from Kim(2017)

The initiative also exhorts comprehensive cooperation among related industries and organizations to defend information and communications infrastructure. Following is the five categories that federal government classified as cybersecurity threats. First, all kinds of law-breakers including offenders who attempt to exploit financial gains. Second, spies including secret agents who aim to steal intelligence assets or conduct cyber espionage. Third, state-affiliated combatants who launch a cyber attack to achieve strategic purposes of their homeland. Fourth, hacktivists delivering cyber attacks with non-monetary rewards. Fifth, terrorist organizations commit internet terrorism. The "Strategy for Operating in Cyberspace" written by DOD in 2011sorted out three offensive actions as adversarial activity. First, cyber activities aim for data manipulation and exploitation. Second, any cyber activities identified as DoS in order to disrupt processing information or operating network-enabled resources. Third, any destructive action including data manipulation, system corruption, and degradation of connected systems.[61]

To sum up, the two prominent focal point of cybersecurity strategy of the US is securitization and militarization.[62] Compared to other countries, the US publicly affirmed that it will assume cyberspace tantamount to traditional realm of national security exemplified as land, sea, and air. The country declares it will take proactive measures against any kinds of APT. The US also ceaselessly attempts to work with like-minded allies for protecting cybersecurity. The country promised to deepen cooperation with other international like-minded partners on cybersecurity-related issues including data preservation, privacy protection, cybercrime, and network defense against cyberattack. To strengthen cooperative ties, the US works closely with North Atlantic Treaty Organization (NATO), especially in concert with UK. Within the Asia-Pacific region, the US works closely with Japan, Australia, and South Korea.

[61] Department of Defense, 2011

[62] Sheen, 2016

2. Information security and regulatory regime

a. Definition of Critical Information Infrastructure

The overall consensus is cyberattack towards both government agencies and private sectors continue to increase exponentially. The total number of reported cyberattack against federal agencies increased from 34,048 to 46,160 –which means, 35% increase between 2010 and 2013.[63] The PwC report published in 2015 traced 42.8million security breach occurred in cyberspace by showing 48% increase in security incidents compared to that of previous report.[64] The US thereby put a great deal of effort in drafting legislations in federal level to enhance infrastructural development. Moving on to Obama administration, the government continued policy guideline from preceding government in a broad sense. Compared to Bush administration, the topic of nontraditional security threat was in the limelight as one of the most imminent national agendas. Among nontraditional security threat, the topic of cybersecurity in relation to safeguarding CII came to the fore. "*Cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.*" Many experts stress the importance of effective cooperation between public and private sector to tackle cybersecurity issue, and therefore the government distributed responsibilities to government-affiliated organizations.

[63] GAO, 2013
[64] PwC, 2015

Table 1. Lists of relevant Federal Agency for CII security and infrastructure resilience

Federal Agency	Area of responsibility
DHS	Estimate security capabilities Develop policy
DNI	Provide information regarding CII threat evaluation
DOS	Protect CII outside of the US Seek cooperation with foreign allies
DOI	Protect government facilities and national monuments
DOC	Facilitate public-private partnership
DOJ	Investigative agency for foreign espionage activities
GSA	Assist and execute a contract for CII
FCC	Identify ICT vulnerabilities Develop priority of ICT-related infrastructure

Note. Adapted from KISA Report

The guiding principle to protect CII and its classification work were completed during Obama administration. Along with abovementioned Presidential Policy Directive 21, the Executive Order 13636 was issued in February, 2013, for the purpose of defending homeland infrastructure system. Following is the major focal point of Executive Order 13636.

Table 2. Main foci of Executive Order 13636

1. Set up an cybersecurity information sharing system		
Detailed subject area	Information sharing	• Information sharing between government-private • Information sharing among CII operators
	Privacy and Civil liberties	• Rule out the possibility of privacy infringement • Implement policy measures to minimize encroachment on a civil liberty
2. Develop cybersecurity framework for CII protection		
• Develop framework under the guidance of NIST • Set up a mechanism, technical standard, and proper procedure		
3. Promote reinforcement program of cybersecurity		
Detailed subject area	Voluntary program	• Promote a practical security • Encourage voluntary security enhancement • Provide incentive program • Competent authorities: DOC and DOT
	High risk group	• Sort out high risk group among all CII • Risk based supervision

Note. Adapted from KISA Report

With no doubt, CII is a backbone to a well-functioning society. Any kinds of cyberattack will be detrimental since this can pose a grave risks on infrastructure resilience. Many countries grapple with devising an agreed framework on CII categorization. Nonetheless, the definition of CII and its categorization vary among countries due to different security environment, objectives, and priorities. Owing to the high reliance on information and communication networks in the US, identifying CII is the first step in building stable homeland cybersecurity. Under the Presidential Policy

Directive 21, Cybersecurity & Infrastructure Security Agency (CISA) categorizes the country's CII into sixteen sectors in total.[65]

Table 3. CII classification system of the US

1	Chemical sector • Basic chemicals • Specialty chemicals • Agricultural chemicals • Pharmaceuticals • Consumer products	5	Dams sector • Irrigate 10% of US cropland • Protect 43% of US population from flooding • Generate 60% of electricity in the Pacific Northwest
2	Commercial facilities sector • Entertainment and Media • Outdoor Events • Public Assembly • Real Estate, Lodging • Retail • Sports Leagues, Gaming	6	Defense industrial base sector • Partnership with DOD • Design, production, delivery, R&D, and maintenance of military weapons
3	Communications sector • Information Technology Sector • Financial Services Sector • Emergency Services Sector • Transportation Systems Sector	7	Emergency services sector • Emergency Management • Law Enforcement • Public Works • Fire and Rescue Services • Emergency Medical Services
4	Critical manufacturing sector • Primary Metals Manufacturing • Machinery Manufacturing • Electrical Equipment, Appliance, and Component Manufacturing • Transportation Equipment Manufacturing	8	Energy sector • Electricity • Oil • Natural gas

[65] Presidential Policy Directive 21, 2013

9	Financial services sector • Depository institutions • Providers of investment products • Insurance companies • Credit and financing organizations • Providers of critical financial services	13	Information technology sector • Hard/software, IT system • Identify threats, assess vulnerabilities
10	Food and agriculture sector • Dependent with many sectors • Water/Wastewater Systems sector • Transportation Systems sector • Energy sector • Chemical sector	14	Nuclear reactors, materials, and waste sector • 99 Active Power Reactors • 18 Decommissioning Power Reactors • 31 Research Test Reactors • 8 Active Nuclear Fuel Cycle Facilities
11	Government facilities sector • Education Facilities subsector • National Monuments subsector • Election Infrastructure subsector	15	Transportation systems sector • Aviation • Highway and Motor Carrier • Maritime Transportation System • Mass Transit and Passenger Rail • Pipeline Systems • Freight Rail • Postal and Shipping
12	Healthcare and public health sector • Dependent on fellow CII sectors • Dept of Health and Human Services designated as Sector-Specific Agency	16	Water and wastewater system sector • 153,000 public drinking water systems • 16,000 publicly owned wastewater treatment systems

Note. Adapted from CISA

b. The evolution of discussion on information security

The country on a surface level seems to be captivated by the aftermath of the September 11, but it goes back many years earlier when the discussion on information security began to loom. Over the time, the country viewed information security in light of cybersecurity with the looming danger from external cyberattack. The evolution of discussion on information security can be organized four periods in a chronological sequence.[66] First period is during the 1990s when the computer technology and relevant businesses enormously expanded.[67] The spread of international network – later shortened to "Internet"– accelerated the notion of cyberspace and free flow of information. The US government exhorted relevant industries to thrive rather than regulated them. In those days, the concept of information security was relatively insignificant and the discussion on security narrowly revolved around monitoring overseas activities.

Second period is during the time of September 11 attacks, which sparked the country to tighten up security-related regulations. The September 11 proved to be a catalyst in stimulating security awareness more than ever. In regard to national security policy, the administration adopted pragmatic approach by appealing to allies. Bush administration successfully proclaimed global war on terror in collaboration with the Pentagon, reestablished relationships with former adversaries during Cold War, and further created allegedly "coalitions of the willing" to grapple with common security agendas through launching proliferation security initiative (PSI).[68] The US assigns multi-layered responsibility to its subordinate organizations and accordingly DHS, DOJ, and DOD emerged as a nascent regulatory body in response to the security attack. As aforementioned, the country appreciated the gravity of the domestic security status since September 11 and thereby a series of relevant security regulations including preservation

[66] Russo, 2016
[67] Crowell, 2016
[68] Trachtenberg, 2004

of homeland information system were carried out.

Table 4. Policy initiatives on information security during Bush administration

Title	Enforcement date	Main point
Executive Order 13228	Oct. 2001	Establish Office of Homeland Security Establish Homeland Security Council
Executive Order 13231	Oct. 2001	Protect CII from cyberattacks
Homeland Security Act	Nov. 2002	Integrate existing departments into DHS
Electronic Government Act	Dec. 2002	Enact Federal Information Security Management Act(FISMA)
Homeland Security Presidential Directive 7	Dec. 2003	Devise a national infrastructure plan
Homeland Security Presidential Directive 23	Jan. 2008	Formulate CNCI

Note. Adapted from KISA Report

The main point of the security discussion focused on protecting social infrastructure and accordingly state-led classification work commenced.[69] Among the relevant regulatory measures, the USA Patriot Act of 2001 permits the use of information sharing between government agencies. The Federal Information Security Management Act of 2002 established a set of guidelines for cybersecurity. The Terrorism Prevention Act of 2004 and Intelligence Reform were also legislated during this period. Above all regional powers in Asia-Pacific, the US watched the rise of China syndrome with keenest interests. Both US media and the Congress have stressed the need for constant vigilance based on the country’s suspicion that China is eager to push the US out of China’s area of

[69] Department of Homeland Security, 2001

influence in Asia.[70] To sum up, during this second period, the country urged the necessity for immediate action in regard to reinforcing protecting internal security and consequently a series of policy initiatives were implemented during Bush administration.

Third period is when the US Office of Personnel Management (OPM) suffered a series of data breaches by external cyberattack.[71] The discussion on cybersecurity in this period mainly revolved around data protection, allegedly protect inside information from any kinds of cyber espionage. Along with ever-advancing technologies represented by APT, the issue of data theft prevails from individual criminal groups to state-sponsored spies. Since the early 2010s, so-called China's threat theory – also known as Chinese conspiracy theory – began to loom inside the US. Obama administration published a series of statement of cybersecurity strategy to make the country's stance clear. Obama administration made it clear that the government will devise a national plan to enhance its security capacity with the help of industry-wide collaboration with relevant federal agencies. The implementation of Cybersecurity Act during Obama administration marks fourth and the last period.

3. Cybersecurity Act of 2015

Protecting homeland CII belongs to nation's vital interests. The Cybersecurity Act of 2015 was included in "Consolidated Appropriations Act 2016," which was signed into law at the end of 2015. The Act is very much known for its first chapter called "Cybersecurity Information Sharing Act (CISA)." The Act first sets forth key definitions.

[70] Limaye, 2004
[71] Washington Post, 2017

"Cybersecurity purpose" refers to any purpose of protecting information asset against internal or external cybersecurity threat.[72] The notion of "security vulnerability" encompasses any attribute of process, software, or hardware that could damage security control.[73] "Cybersecurity threat" refers to an action towards information system that may adversely affect the security, availability, or integrity of data.[74] "Cyber threat indicator" coined in this Act means identified malicious reconnaissance activity and suspiciously identified anomalous communication patterns that appear to be relevant to cybersecurity threat.[75] "Defensive measure" refers to an action, procedure or technique applied to information asset in an attempt to detect and mitigate security vulnerability along with cybersecurity threat.[76]

The essence of the Act is to promote information sharing between the nonfederal and federal government agencies to bolster homeland cybersecurity. The Act stipulates the corresponded subjects with obligation required to meet the goal of desirable information sharing, the kinds of information they need to submit, and the according procedures. Federal government agencies concerning the Act – the DNI, DHS, DOJ, and DOD – shall cooperate with relevant entities in developing defensive procedures and should promulgate measures.[77] The content of unclassified cyber threat indicators shall be timely shared between federal government and relevant entities in an

[72] 6 U.S.C. §1501(4)
[73] 6 U.S.C. §1501(17)
[74] 6 U.S.C. §1501(5)
[75] 6 U.S.C. §1501(6)
[76] 6 U.S.C. §1501(7)
[77] 6 U.S.C. §1502(a)(1)

attempt to prevent adverse effects.[78] Abovementioned procedure shall be submitted and shared in a voluntary manner.[79] To encourage voluntary participation, the Act provides grounds for immunity from legal responsibility.[80] The Act publicly clarifies that information sharing procedure is conducted in neither compulsory nor forceful manner. The Act is rather based on the principle of voluntary participation. Although corresponding entities are bound to engage in information sharing, there is no liability for not participating in this voluntary activity.[81]

The Act also elucidated how the federal government entities will use the gathered information. With the written consent of an authorized federal entity, information system of private entity can be monitored and shared in the name of cybersecurity purposes.[82] The Act clearly specifies that cyber threat indicators and defensive measures shared between federal government and private entities will not be disclosed to the general public.[83] The Act lastly specified how government activities will be supervised according to the law. The Act rules out the possibility of sharing personal information illegally. Any information containing personal or irrelevant information will be ruled out during a sharing procedure among relevant entities.[84] The Act also pronounces that reviewing process will be proceeded to censor any content irrelevant and to eliminate such information.[85]

[78] 6 U.S.C. §1502(a)(4)
[79] 6 U.S.C. §1504(c)(1)
[80] 6 U.S.C. §1505(b)
[81] 6 U.S.C. §1507(i)
[82] 6 U.S.C. §1503(a)
[83] 6 U.S.C. §1504(d)(3)
[84] 6 U.S.C. §1504(a)
[85] 6 U.S.C. §1503(d)

IV. China

1. An overview of national security and network security

a. The development process of informatization

Ever since the mid-1990s, China has been conducted comprehensive research and put enormous resources to develop its information technologies under the goal of creating an information society. To build an information society, China initiated ICT-centered development plan at national, provincial, and municipal level. Focused on e-development framework concept including e-government, e-rural, e-business, and e-community, ICT serves as enabling force in achieving country's national goal. China's ICT development plan is in the form of long-run investment strategy, both financed and controlled by the central government.[86] The impetus for China's informatization strategy is based on a shared belief among the political entities that ICT advancement will enable China to open up new growth opportunities and to reform industries fundamentally. With this shared belief, the Chinese government itself acted as leading role in encouraging the diffusion of internet and e-commerce. To fully enjoy the benefits from ICT revolution, China attempted to invest further in a chain of reforms including policy reform, governance reform, and institutional structure reform.

The CCP embarked on a series of state-run projects called Golden Project (金盾工程) in March 1993 in the progress toward moving into market economy. The Golden Projects, comprised of both first-tier and second-tier plan, was designed to boost

[86] Hanna, 2018

informatization and economic growth.[87] Subsequently, the Golden Project placed priority in sector-specific format such as government portals, tax administration, online transactions, and payment systems. In addition, development projects per industry – insurance, health, agriculture, and tourism – proliferated during this period. The year 1994 marked the time when the country introduced international network – later called internet –on a nation-wide scale and launched comprehensive national work on China National Information Infrastructure (CNII) development, represented by policy reform under the State Council, national campaigns including Golden Project.

The National Information Development Plan drafted in 1997 elucidated informatization plan along with regulations applicable to network infrastructure, information resources, and relevant industries. Political elites in China at the time desired to promote the country's advancement under the name of informatization strategy while at the same time hope to maintain their power and influence. The establishment of China Internet Network Information Center (CNNIC) in 1997 indicates China's commencement of systematic internet governance. In the same year, national informatization conference was held for the first time and relevant set of regulations applicable to information technology, industry, networks, and human resources were also outlined by the government.[88] As an indispensable element of CII, China has been expanded the internet industry under the state-led information policy. The authorities later promulgated "Government Online Project (政府上网年)" in November 1998, saying that 60 percent

[87] Hanna et al, 2010
[88] Kam et al, 2002

of government offices and 80 percent of national ministries will go online by the end of 2000.[89] China even called the year 1999 as "The Government Online Year" and embarked upon "Enterprise Online Project" in the year 2000.

China assumed investing in ICT is prerequisite for informatization along with industrialization, which will bring country's economic development in the end. The unfettered use of internet in China, however, has been challenged because of political propaganda from Western countries. For that reason, Chinese authorities were eager to regulate and control the public use of internet. To understand the political impact of internet on Chinese society, it is important to comprehend how the internet is perceived and governed inside China. Since its earliest inception, the internet governance can be explained into three stages, which are experimental period before 1994, transitional period ranged from 1994 to 1997, and the latest period since 1998. Under the name of Golden Projects, China sought digitized communications and advanced network system in governmental agencies, and financial institutions. Added to this, the allegedly nine information categories made by Chinese central government were banned for creating and transmitting in the Internet.[90]

First, any content that degrade the basic principles stipulated in the Constitution

Second, any content that imperils national security and jeopardizes national unity

Third, any content that undermines the state's interests and prosperity

Fourth, any content that evokes ethnic solidarity and ethnic animosities

Fifth, any content that impedes state's religious policies

[89] Cheng, 2012

[90] IGI Global, 2009

Sixth, any content that sabotages social order and social stability

Seventh, any content that instigates obscenities including terror and violence

Eighth, any content that infringes legal rights of others

Ninth, any content that includes prohibited contents written in administrative regulations

b. Cybersecurity strategy guideline

China stipulates protecting mainland cybersecurity as a matter of grave importance to the prosperity of a nation. The "National Cyberspace Security Strategy (国家网络空间安全战略)" formulated by CAC identifies objectives, opportunities, strategic tasks, and challenges in pursuing Chinese cybersecurity strategy. The cyberspace security strategy identifies five objectives, which are peace, security, openness, cooperation, and fair order in cyberspace. Following is four guiding principles; first, respect and protect sovereignty in cyberspace; second, champion the peaceful use of and in cyberspace; third, govern cyberspace abide by the relevant law; fourth, implement comprehensive regulation on cybersecurity and cyber capabilities development. The strategic paper also elaborates seven development opportunities that impel China to invest enormously in protecting cybersecurity and developing relevant technologies. First, cyberspace will serve as a new, effective channel for information dissemination. Second, cyberspace will become new frontier of people's life. Third, cyberspace will function as driving force for national economic development. Fourth, mature cyberspace environment will bring Chinese cultural prosperity. Fifth, cyberspace will function as principal means of social governance. Sixth, cyberspace is a new mode of cooperation and interaction. Seventh, China endorse cyberspace as new domain under the influence of Chinese sovereignty. Following is the nine strategic tasks; first, defend Chinese sovereignty in cyberspace; second, defend national security; third, safeguard critical information infrastructure' fourth, build healthy cyberspace environment; fifth, combat cyber crime including internet terrorism and cyber espionage; sixth, develop good cyberspace governance; seventh, enhance cybersecurity capability; eighth, elevate cyber defense capabilities; ninth, seek international cooperation. The five grave challenges, which Chinese authority began to grapple with, are system penetration, cyber theft, any erroneous information up in the internet, online terrorism through internet propaganda, and international competition which brings needless competition.[91]

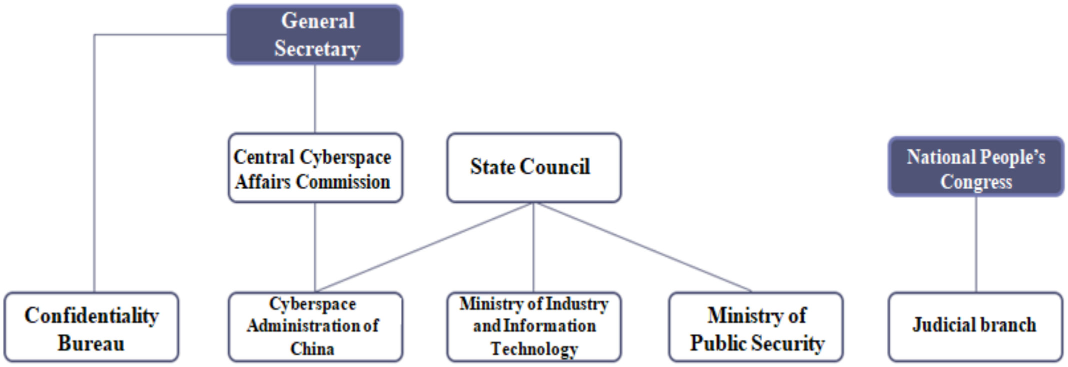
China publicly upholds the idea that every country's national security, issue of sovereignty, and development interests are at stake owing to the growing seriousness of cybersecurity. Accordingly China issued another official document "International strategy of cooperation on cyberspace (网络空间国际合作战略)" which implies Chinese wishful thinking of international cooperation in advocating healthy cyberspace. The document contains basic principles, strategic goals, and plan of actions. While abovementioned document narrowly focused on cybersecurity strategy aims to operate inside China, this document demonstrates China's viewpoint on international cooperation to ensure common interests regarding cybersecurity. China established four basic principles regarding international cooperation in cyberspace, which are principle of peace, sovereignty, shared governance, and shared benefits. Following is six strategic goals

[91] Washington Post, 2017

which all nations should cooperate for shared interests in cyberspace; first, respect cyberspace sovereignty; second, develop international rules; third, pursue fair internet governance; four, promote citizen interests and rights; fifth, promote international cooperation for digital economy; sixth, build platform for cultural exchange between countries. Lastly, China urges global cooperation by publishing a nine slogan – first, peaceful and stable cyberspace; second, rule-based international order applicable to cyberspace; third, intra-country partnership; fourth, reform internet governance system; fifth, international cooperation for combating cyber crime; sixth, protect citizen's rights and interests; seventh, invigorate digital economy; eight, develop global information system; ninth, share each one's cyber cultures.

Last but not least, China employs top-down approach to implement the country's proposed cybersecurity framework. Following is the organizational structure of China to defend mainland cybersecurity.

Figure 4. Organizational chart of Chinese cybersecurity


General Secretary
Central Cyberspace Affairs Commission
State Council
National People's Congress
Confidentiality Bureau
Cyberspace Administration of China
Ministry of Industry and Information Technology
Ministry of Public Security
Judicial branch

Note. Adapted from Ministry of Public Administration and Security

Central Cyberspace Affairs Commission under the General Secretary was installed in February 2014 to take overall responsibility in terms of internet control and cybersecurity management. The CAC functions as a working-level agency. The Ministry of Public Security (MPS) takes in charge of confidential information protection. Ministry of Industry and Information Technology (MIIT) seeks development of equipment and country's informatization. The National Computer Network Emergency Response Technical Team/Coordination Center of China (CN-CERT) under the MIIT detects cyber threats and performs cybersecurity-related missions. Confidentiality Bureau conducts security inspection and formulates cybersecurity-related policy.

2. Network security and regulatory regime

a. Cybersecurity environment

China only recently embraced the internet in 1994 and thereby examining Chinese internet environment needs to be preceded before gauging China's holistic cybersecurity environment. The cyber environment in China indeed has some globally shared international features, but at the same time it possesses Chinese distinct characteristics. Compared to that of other countries, Chinese internet has somehow been domesticated based on the country's inherent nature.[92] Under the government regulation, the internet network service is mainly operated on a corporate level for the sake of making profits. Ever since the government officially launched informatization plan in the 1990s, contents in the internet has been monitored. The authority put forth a special effort to control free flow of information within the mainland and block information

[92] Yang, 2012

content from spreading outside of China. The "Great Firewall", an internet control system, was formed to deliberately separate the country's virtual boundary in cyberspace from the outsider.[93] China's internet censorship policy plays a leading part in governing society, advancing the state power over the cyberspace, and securing economic profits from the booming internet-mediated industry.

The chief end of cybersecurity regulation shifted from peripheral control of internet network to direct censorship on information from mid 1990s to 2010s.[94] Consequently, China launched a comprehensive cybersecurity inspection on network systems operating key industries and government ministries since 2014. The establishment of internet governance organization Cyberspace Administration of China (CAC, 国家互联网信息办公室) adds a dimension to the national goal of becoming a leading country in terms of cybersecurity.[95] When China first introduced internet in 1994, the country's priorities were limited to industrial development, infrastructure reconstruction, and forming systemized information system. From then on, China expanded its area of regulation up to internet governance. The main focus of CAC inspection revolves around CII protection. Under the nationwide CAC inspection, more than 31 provinces and 54,000 information systems were monitored.[96]

To sum up, the censorship practice indicates China's precaution against any kinds of adverse consequences resulted from using internet. It corresponds to the country's

[93] Bloomberg, 2018
[94] Li and Robbin, 2013
[95] Miao, 2016
[96] Chinese Academy of Cyberspace Studies, 2018

national strategy goal of maintaining “stability (维稳)”. The authority’s basic stance in controlling mainland cyberspace environment is that inspection should be intensified to discern not only cybersecurity risks, but loopholes of Chinese cyber capabilities which pose threat to national security. After Xi Jinping assumed leadership, the country puts spurs to internet governance stresses the notion of good governance in cyberspace which directly affects national internets and regime security.[97]

b. Definition of Critical Information Infrastructure and regulatory regime

For a lengthy period of time, China has been underwent a series of disputes among political elites regarding the range of CII protection and categorization. Among others, Xi Jinping asserted that what the country meant by safeguarding mainland cybersecurity is to protect CII. Under the leadership of Xi Jinping, the CAC works as a leading body for CII regulation and China established a standard upon CII protection. CII identification in China follows three steps.[98] Step one of CAC guideline is identification of Chinese critical sectors. Step two is to identify industrial control system and/or information systems operating CII. Step three aims to identify the potential loss or damage due to cybersecurity breaches. There are a total of twelve CII sectors in China.

[97] Xinhua News, 2015
[98] The Diplomat, 2018

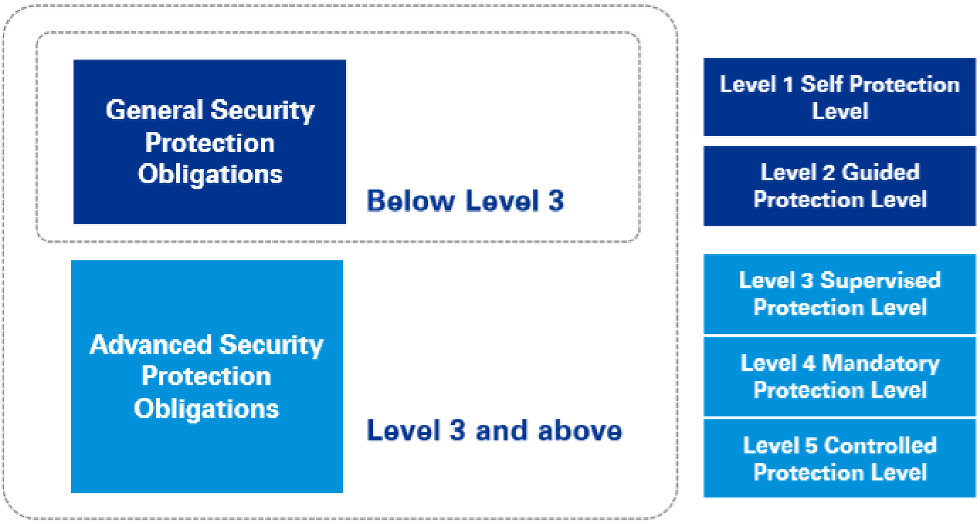
Table 5. CII classification system of China

1	Energy sector •Electricity industry • Petrochemical industry • Coal industry	7	Industrial manufacturing sector • Enterprise management • Smart Device (IoT) • Harmful chemical substance
2	Finance sector • Banking system • Securities and futures • Electronic liquidation • Insurance regulation	8	Telecommunications and internet sector • Internet domain name registration • Data center, Cloud service • Basic Network Information center
3	Transportation sector • Railway, Expressway • Aviation • Water transportation	9	Broadcasting and television sector • Television industry • Broadcasting system • Disciplinary action
4	Water conservancy sector • Water resources development • Supply of water • City water authorities	10	Municipal administration sector •City water system • District heating system • Wastewater treatment system • Smart City management
5	Healthcare and hygiene sector • Public health agency • Disease management • Regional emergency centers	11	Government sector • Freedom of Information • Public service • Office business system
6	Environmental protection sector • Environmental monitoring • Early warning system • Nuclear power plant system	12	Others • Other sectors in all social strata

Note. Adapted from CAC

Along with the CAC guideline, “Administrative Measures for Information Security Multi-Level Protection Scheme (MLPS)” by the MPS is another important regulatory regime. MLPS system elucidated how China seeks to protect domestic CII. While the CAC guideline focuses narrowly on CII protection, the MLPS covers whole range from CII to general network system operators including big data centers, industrial control systems, mobile internet enterprises, and public service platforms. The MLPS regulation asks every network operators in China to classify their network system under the five-level system. The corresponded subjects and/or network operators should comply with MLPS code of conduct and the authority’s security inspection based on their designated security level.

Figure 5. MLPS five-level system


General Security Protection Obligations
Below Level 3
Advanced Security Protection Obligations
Level 3 and above
Level 1 Self Protection Level
Level 2 Guided Protection Level
Level 3 Supervised Protection Level
Level 4 Mandatory Protection Level
Level 5 Controlled Protection Level

Note. Adapted from KPMG China

Within the five level systems, below level three are the subject of general security protection obligations. Level three and above should follow advanced security protection obligation. The MLPS regulation issued by MLPS and the CII regulation laid out by the CAC are the two most important supplementary regulations for the CSL.[99]

3. Cybersecurity Law of the PRC

The Cybersecurity Law (CSL) implemented in 2016 first clarifies significance and purpose of establishment. CSL is promulgated for the purpose of protecting Chinese network security, safeguarding sovereignty in cyberspace, promoting sound cybersecurity environment, and ultimately preserving public and national interests.[100] Under the law, the State equates the need for network security with the development of ICT.[101] CSL put emphasis on disseminating cardinal values of socialism to corresponded subjects thereby asking corresponded subjects to follow the network practices under the socialist system.[102] Last part of the first chapter reconfirmed that every corresponded subjects including private entities and state enterprises should abide by the Chinese Constitution along with social order.[103] Corresponded subjects shall seek to discern any behavior in cyberspace that aims to discredit the state power, instigate extremism inside the country, or fabricate false information in cyberspace.

CSL categorized network operators, illegal program, network security, key information infrastructure to enhance the efficiency and control. The CSL clarifies what kinds of information that the authority aims to protect. The CSL stipulates in what manner the relevant authority including State Council and competent departments plan to regulate information sharing inside China. The State Council implements the “Network

[99] KPMG China, 2017
[100] CSL, 2016, Article 1
[101] CSL, 2016, Article 3
[102] CSL, 2016, Article 6
[103] CSL, 2016, Article 12

Security Classification System" as a regulatory framework. Network operators assume an obligation stipulated in classification system (MLPS) to protect systems from any kinds of external disruption, unauthorized access and malicious interference.[104] CSL further specifies mandatory requirements which network products and services should comply with. Providers of abovementioned network systems and services shall not install malicious programs, notify the users whenever asked to do so, and submit report to the State Council along with competent authorities.[105] The information sharing process adopts coercive measures together with punishment system. Accordingly, the CSL clarifies lists of legal liability in case of non-compliance with the law.

Finally, the CSL rules out the possibility of privacy infringement. The law bans network operators from disclosure or alteration of personal information unless prior consent is guaranteed by corresponding citizen.[106] Network operators shall cooperate with the State Council in implementing the CSL. If any individual or private group feels uneasy about the network operators' use of such information –for example, in case of network operator violates the provisions of law –then corresponding individual is entitled to ask network operators expunge their personal information.[107] Therefore, both private entities and state enterprises shall not obtain, sell, or distribute citizens' personal information in an unfair and unjust manner.[108] More than anything, the CSL strongly asks competent authorities to observe confidentiality regarding business secrets and

[104] CSL, 2016, Article 20

[105] CSL, 2016, Article 21

[106] CSL, 2016, Article 41

[107] CSL, 2016, Article 42

[108] CSL, 2016, Article 43

personal information obtained during the procedure.[109]

V. Analysis

1. Thesis findings

What previous studies have demonstrated is both well appreciate the magnitude of cybersecurity and this so-called G2 work as a pioneering countries in developing cybersecurity protection scheme. Following is the direct comparison of Cybersecurity Act of 2015 in the US and Cybersecurity Law of the PRC implemented in 2016.

Table 6. Direct comparison table of cybersecurity legal regulation

	Cybersecurity Act of the 2015	**Cybersecurity Law of the PRC**
Corresponded Subject	Private entities	Network operators CII operators
CII categorization	16 CII sectors	12 CII sectors
In case of non-compliance	No punishment	Fine, penalty
Relevant Organization	Relevant federal agencies (DNI, DHS, DOJ, DOD)	CAC and the Central government
Operating Method	Information sharing (Share cyber threat indicators)	Submit security inspection results (according to MLPS system)
Implementing Principle	Voluntary participation basis	Compulsory provisions with punishment system
Personal Data Exclusion	Review procedure	Corresponded subject shall send notification to individual

[109] CSL, 2016, Article 44

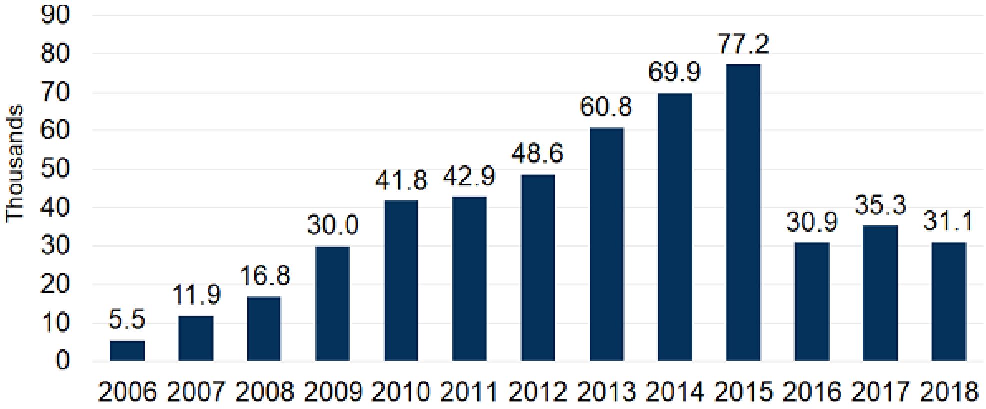
On a closer view, both legal regulation shares one common dilemma which refers to the possible danger of surveillance owing to blurred demarcation between the concept of cybersecurity and personal information. Whether it is old democracies or new, all of them have witnessed remarkable development of surveillance technologies and cyber capabilities in recent years. In the most advanced democratic countries like that of US, there is possible danger of advanced surveillance technologies be deliberately manipulated for the purpose of information gathering. Meanwhile, in countries with young democracies, there is a danger of excessive surveillance and spying technologies being used to extend their repressive power at the expense of personal privacy and security. Thus the danger of mass surveillance technique is that nation can pose a threat to individual privacy and/or freedom, disregard rule of law. In today's cyber era, many experts express concern about the regression of democracy due to digital sabotage, especially regarding the possibility of internet – using its innate nature of anonymity and indefensible topography – becoming a cornerstone medium that brings trans-border digital sabotage activities.

Nonetheless, the fundamental purpose for implementing legal regulation is to protect domestic information security and ultimately building a mature cyberspace in its own way. The underlying reason why the US and China advocate different legal approaches is attributable to security perception of traditional security and social priority. Different security perception applied in traditional security realm is reflected upon cybersecurity field. Added to this, the statute also demonstrates different prioritized values advocated by respective country. In the following subchapters, different protection scheme, pressing concerns, and further implications will be covered in detail.

a. The US model of protecting homeland cybersecurity

As former director of the DNI James Clapper once commented, the US assumes cybersecurity threat as imminent national security matter ever since the September 11. The country propagates seriousness of homeland cybersecurity, the need for consolidating federal authority's governing power, and thereby Cybersecurity Act of 2015 was implemented. As stated above, two main variables – perception of traditional security and prioritized social value – are mirrored in the Act. The security perception stipulated in the Act is in line with the country's long-held national security beliefs and standpoint. The core security vision of the US is the renewal of American leadership in the 21st century. To keep good status as a world hegemon, the US assumes defending the country's information security amid proliferated cyber threats. The enforcement date of Act coincides with the time when the US publicly announced the era of Asia-Pacific under Obama administration with its strategy known as Pivot to Asia. China, with no doubt, is the most fast-developing country in terms of ICT and cyber capabilities. After a succession of cybersecurity damage later identified as China-based deed, the Act takes a firm stand against any kind of external cyberattack. The country's long-cherished social priority also wielded influence on the Act. With the introduction of internet, the country underwent unceasing trial and errors. Respect for individual freedom and free flow of information are the two most dominant social values pertaining to the US model of cybersecurity. Thus protect individual privacy and safeguard intellectual property are core priorities stipulated in the Act. On the downside, the dilemma of the Act is low participation rates and continuous dispute on infringement of personal data. The allegedly Snowden incident in 2013 sparked the discussion regarding excessive surveillance conducted by the authority. Added to this, the nature of infrastructure as a public good impedes law enforcement since the problem of free-rider remains unsettled. In the face of widespread criticisms, the US witnessed relatively good results after the enforcement of the Act. According to the OMB, the number of cyber incidents reported by federal agencies decreased after the enforcement of the Act in 2015.

Figure 6: Incidents Reported by Federal Agencies to US-CERT



Note. Adapted from OMB

To sum up, the viewpoint on traditional security in the US and the country's long-held social value contribute in developing the US model of protecting homeland cybersecurity. The main foci of the Act are renewal of CII, build safe and sound information circulation within the country, and defend inside information from any kinds of external cyber threats.

b. Chinese model of controlling mainland network security

China places emphasis on cybersecurity in earnest since Xi Jinping assumed power. The CSL well manifests the country's perception of national security agenda which is upholding the country's identity under the communist regime. Chinese cybersecurity model adopts entirely top-down governance style and penal regulation. If the corresponded subjects – without reference to domestic enterprises or foreign firms – violate the law, it will be punished by law. The CSL asks interested parties to abide by the law in a compelling way. Unlike the US model of cybersecurity legal regulation, CSL advocates the concept of cyber sovereignty which refers to respecting every country's sovereignty in cyberspace under the principle of non-intervention. In addition, Chinese prioritized socialist value is deeply entrenched in the CSL.

> "*Article 1: Socialist State. First, the PRC is a socialist state under the people's democratic dictatorship led by the working class and based on the alliance of workers and peasants. Second, the socialist system is the basic system of the PRC. Sabotage of the socialist system by any organization or individual is prohibited*."
>
> *– Cybersecurity Law of the People's Republic of China 2016*

Meanwhile, many express concerns that unclear sub-clause and broadly defined technical terms leave too much room for interpretation. Experts view CSL intentionally adopted broadly defined language in order to let CAC along with relevant authorities to easily regulate information circulation inside China and wield power.[110]

[110] Ropes & Gray. 2017

2. Implications and prospects of nations in the cyber era

a. Cybersecurity as a shared problem

When viewing the prospect of nations in the cyber era, one important thing to be noted is cybersecurity after all is a matter for every country. To put it simply, it's a shared problem. Given all possible cyber threats in a myriad of ways, every country have been concurred with having international cooperation to mitigate dangers such as cyber crime, cyber espionage, internet terrorism, or data interception. Apparently, a number of multilateral cooperation initiatives are underway in order to tackle cybersecurity as everyone's shared problem. Following three cases are the most well-known and active multilateral efforts to combat cybersecurity threats.

First one is Internet Governance Forum (IGF). The IGF functions as the most high-level dialogue regarding global internet governance. The latest 12th IGF entitled "Shaping Your Digital Future" was held in Geneva in 2017. Cybersecurity-related topics including digital economy, internet governance, ICT development goals, AI, digital literacy and information acquisition were covered in the forum.[111] IGF is actively working in conjunction with field experts by holding regular Multi-stakeholder Advisory Group (MAG) meeting.

Added to this, the United Nations is engaging in this relatively new security realm. The UN Group of Governmental Experts (UNGGE), composed of experts in field of science and computer security, was established in 2004 with the goal of developing appropriate measures and helping governments to work better in cyber space. At present,

[111] Chinese Academy of Cyberspace Studies. 2020

the UNGGE is the largest multilateral cooperation organization for cybersecurity. With the goal of establishing international regulations to defend member states' information and cyber security, the UNGGE provides a place to discuss cooperation schemes. The second UNGGE (2009-2010) talks concentrated on ICT utilization standard in a discussion. The member of the expert group discussed cyber-related agendas such as risk reduction actions for ICT-related discord situation, confidence-building measures, and capacity-building for developing countries.[112] The third UNGGE in 2013, in particular, acquired importance in the sense that it reached an important agreement. The governmental experts agreed upon ICT agenda that using ICT is permissible as a means to achieve a country's specific goal under the International norm stipulated in the UN Charter. Subsequent meetings in 2014 and 2015 focused on how internationally agreed code of conduct could be applied given the basic principles underpinned by international law such as national sovereignty, the right of self-defense, and humanitarian law. Although declaring the right to self-defense is customary law in international law, both Russia and China denounced strongly because of the possibility of weaponizing cyber capabilities. At the latest UNGGE, governmental experts from total of 25 countries participated. Governmental experts from P5 nations participated in all of the five sessions. As an only multilateral cooperation organization, UNGGE contributed in establishing international legal order for safe and peaceful cyberspace.

Third one is called Shanghai Cooperation Organization (SCO). The SCO was conceived in an attempt to strengthen regional cooperation regarding emerging security

[112] Park, 2018

realms including cybersecurity. The SCO has multi-faceted structure with three cooperation pillars, which are security and political realm, economic and trade realm, and cultural development. The latest summit was held in Qingdao, China, in July 2018. The SCO adopts consensus-based decision making process. Cybersecurity with respect to counterterrorism and cyber theft are the main concern of SCO. The counterterrorism agency council under the SCO, for example, started joint exercise in 2017. Eight member states along with the delegations of competent authorities participated in the exercise for the sake of facilitating information sharing among SCO member states.

Despite growing awareness on cybersecurity and ongoing multilateral efforts, critics argue that economic disparities between the developed and the developing countries hinder countries from furthering cooperation initiatives. Critics argue that those of less developed countries are lack of resources and/or relevant capacity to combat non-traditional security threats spring from cyberspace. They pinpoint the lack of partnership between the rich and the poor countries could bring precarious situation in cyberspace which implies cyber criminals take advantage of legal loopholes. The lack of security measures also could generate developing countries to commit more cybercrimes. Added to the discord between the developed and the developing countries, the discrepancies of opinion emerged between Western bloc and non-Western bloc – mainly China and Russia – are prevalent when looking at a series of multilateral initiatives on cybersecurity. On closer inspection, the landscape of cybersecurity cooperation – especially how UNGGE and operate per like-minded group of member states – reflects cooperative politics in terms of traditional security realm. The SCO, for example, is unique in the sense that the member states are geographically clustered around Asia thereby creating a certain fellowship and ideological similarity.[113] A sense of ideological similarity facilitates in advancing political dialogue regarding discussing cybersecurity.

b. Race to cyber supremacy

Cyberspace is cross-border in essence and compared to that of physical territory under the traditional standpoint, the so-called cyber territory is amorphous. Unlike the times of Cold War where dichotomous thinking between the US and Soviet Union prevailed, today's cyber era is comprised of multilateral parties including both nations and non-state actors. This peculiarity brings controversy regarding enforcement of relevant international norm and effectiveness of government regulation in their respective country in cyberspace. Unlike traditional security environment – land, sea, and air, cyberspace is much more complex and open-ended. Nonetheless, the current cybersecurity landscape is apt to becoming more like countries eagerly investing in cyber capabilities to bolster their own national security. More than any other country, the US and China are two pioneering countries vying for cyber supremacy.

In case of US, the country continuously checks China by referring to recent Chinese inclination for weaponizing cyber capabilities. China, with no doubt, is the country which poses greatest threat to national security of the US. What worries the US is China launching a cyberattack for the purpose of holding US economy as a hostage and jeopardizing US society at large in the face of allegedly the US-China competition. The US criticizes China's offensive action in cyberspace, which is exemplified by

[113] Alimov, 2018

reckless cyber espionage and computer hacking. By invoking international cooperation for cybersecurity, the US makes an objection to Chinese stance on cyberspace which is the principle of cyber sovereignty and non-interventionism. China, on the other hand, denounced the pro-American cyber environment holistically by arguing the predominant position (优势) of the US in areas of technical standards. China purports that current cybersecurity environment is operated under the US cyber hegemony (网络霸权).[114] As a matter of fact, most of software, servers, and routers that China adopted originated from US-based firms.[115] On top of this matter, Chinese observers pointed out the fact that domain name system server under the jurisdiction of Internet Corporation of Assigned Names and Number (ICANN) belongs to US. China claims that ICANN should be transformed into the kind of international organization thereby China could exert equal influence like that of US.[116]

Despite a series of multilateral cooperation to combat rising security threats in cyberspace, recent propensity of cybersecurity environment in the end will bring another version of cyber arms race. Arms race spring from a mutually insecure situation characterized as competitive and mutual-buildup of security capabilities between states. Unlike the conventional weaponry used in traditional physical warfare, weapons in cyber domain are computer codes – all those malware that is made to inflict harm. Given this, it is much more difficult for states to detect and picture counterpart’s capabilities compared to the past when it was physically visible and easily detectable. Furthermore the nature of

[114] Chong, 2010
[115] Guo, 2013
[116] Jian, 2013

anonymity in cyberspace contributes to the sense of uncertainty. Building up cyber technologies, so-called security capabilities in cyber age, is much cheaper than equipping conventional weapons and thus not only developed countries but also weaker countries can possibly participate into the cyber arms race and compete among the rest.

To sum up, recent propensity of cyber governance under the respective country's sovereign power in the end will produce another version of cyber race. In geopolitical standpoint, the so-called G2 are the most active actors in the race to cyber supremacy. The US contains Chinese offensive move in cyberspace and deprecates China's dogmatic approach such as non-intervention in cyberspace along with its recent inclination for weaponizing cyber capabilities. China, meanwhile, denounces present status of cybersecurity landscape by arguing current cyber-related industry is lopsided and international cooperation structure is pro-American. When taking a closer view, however, the chances are in favor of smaller states to gain dominance in cyberspace than developed countries owing to the nature of cyberspace exemplified by low entry barriers and anonymity. There has been an upsurge in weaponizing cyber capabilities among not just advanced countries but developing countries in the name of protecting domestic cybersecurity against external cyber threats. Regarding the race to cyber supremacy, what is clear is cyber arms race will not serve as the final arbiter of power struggle among states, and thus it should not be viewed aside from conventional forms of political violence. In most cases, the efficacy of internet coercion will come into force if only cyberattack is accompanied by other actions including terrestrial military force. Thus, the prospect of nations in cyber era is not just complex but hard to count on peaceful accord through international cooperation.

VI. Conclusion

The advancement of ICT unlocks all possibilities, and thereby makes physical border insignificant. The more the cyberspace continues to evolve with the advancement of relevant technology, the more it is exposed to vulnerability. This study aims to demonstrate how states interact in cyber era. At the outset, nations well appreciate the seriousness of global cybersecurity. Every country has confirmed agreed perception of burgeoning attacks in cyberspace and endorsed collective initiatives to combat cyber threats. Although nations will actively interact and engage in collective initiatives fueled by the rising voice of forming global governance for cybersecurity, the overriding state sovereignty in the end will breed discord. The topic of global cybersecurity become salient, nonetheless, nations become more nationalized in the cyber era. Thus the crux of controversy begins when a country utilizes cyber capabilities to bolster one's national interests. This study acquires importance since it adds a dimension to current cybersecurity studies by focusing on the issue of cyberspace governance in relation to state sovereignty. With that in mind, the study chooses the US and China. By conducting a comparative study on Cybersecurity Act of 2015 in the US and Cybersecurity Law of the PRC in 2016, the study demonstrates how each country implements legal regulation in an attempt to protect domestic information security while exerts its national interests in today's cyber era.

In case of US, the impetus to implement Cybersecurity Act springs from country's concern on CII protection. If anything, the high dependence on networked ICT to facilitate country’s CII will create vulnerabilities which can be exploited by malicious attack. The Cybersecurity Act of 2015 reflects well the security perception of US and it prioritized values. The US adheres to its long-held security vision of renewing American leadership in the 21st century and furthering its international position. The prioritized values exemplified by free flow of information and privacy rights have the upper hand than the country’s longing for regulating homeland cybersecurity environment. When viewing the US model of protecting homeland cybersecurity in a broad sense, the country asks like-minded partners for further cooperation. China, on the other hand, has been concerned over its network security ever since it opened up internet to the general public in 1994. The main concern over Chinese cybersecurity is centered on high dependence on foreign technology and its relatively short history of networked society. By implementing the Cybersecurity Law, China aims to regulate information flow in much more comprehensive manner. Unlike that of the US, the CSL adopts penal regulation thereby corresponded subject will be punished in case of non-compliance. The authority plays a leading role in protecting mainland cybersecurity. The main goal of Chinese model is to build a stable cybersecurity environment for the sake of defending national security. Added to this, China’s basic stance on cybersecurity revolves around advocating cyber sovereignty, which basically appeals the principle of non-intervention.

Studying two countries’ legal regulation vis-à-vis cybersecurity implies a lot when prospecting the future of nations in the cyber era. The study suggests two implications. First, the topic of cybersecurity inextricably is a matter for all countries since the peculiarity of cyberspace such as openness, anonymity, and hyper connection could easily trigger illegal activities. The multilateral initiative on cybersecurity will be in progress. Nonetheless, regulating global cybersecurity through international norm is the conundrum owing to conflicting interests among participating nations. The Sino-US hegemonic competition witnessed in seeking international cooperation is typical example. By that sense, secondly, the allegedly race to cyber supremacy could occur. The US and China are two pioneering countries vying for cyber supremacy.

In the virtual world like cyberspace, actors are anonymous, physical distance is null, and conducting a virtual offensive act requires small budget when compared to that of conventional security environment. Unlike traditional security realm, cyberspace is much more unmanageable and risky when it comes to achieve dominance. Given the past decade, most of the extensive state-sponsored cyberattack are followed by military attack. Compared to the traditional security realm, the cyberattack per se produce only consequential damage. The power of cyberattack, however, will be doubled when combined with kinetic warfare. To conclude, the issue of global governance for cybersecurity and state sovereignty is important to predict the future of nations in the cyber era. Although states will actively interact and engage in collective initiatives, the overriding state sovereignty will add a dimension to this complex cybersecurity landscape. Cyberspace, with no doubt, will neither abolish geographical space nor belittle state sovereignty. Thus, considering traditional security interests plays a pivotal role in picturing the future of cybersecurity landscape since respective state’s sovereignty still play a major role in cyberspace.

Bibliography

Academic Journals:

Alimov, Rashid. "The Shanghai Cooperation Organisation: Its role and place in the development of Eurasia." *Journal of Eurasian Studies,* no.9 (2018): 114-124.

Chung, John. "Critical Infrastructure, Cybersecurity, and Market Failur." Oregon Law Review, no.96 (2018): 441-476.

Craig, Anthony and Brandon Valeriano, "Conceptualising Cyber Arms Race." *IEEE Proceedings for CCDCOE CyberCon,* (2016): 141-158.

Denning, Dorothy. "Framework and Principles for active cyber defense." *Computer& Security*, no. 40 (2014): 108-113.

Eastman, James. "Avoiding Cyber-Pearl Harbor." *The Columbia Science & Technology Law Review,* no. 18, (2017): 515-553.

Ford, Christopher A. "Ending the Strategic Holiday: U.S. Grand Strategy and a "Rising." China." *Asia Policy*, no. 18 (2014): 181-189.

Hanna, Nagy and Christine Qiang, "China's Emerging Informatization Strategy." *Journal of the Knowledge Economy,* no: 1 (2010): 128-164.

Hanna, Nagy. "Why a Holistic E-Development Framework?." *Information Technologies and International Development,* no. 4 (2018): 1-7.

Harknett, Richard and James Stever, "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen." *Journal of Homeland*

Security and Emergency Management, no.6 (2009): 1-14.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security*, no. 2 (2013): 7-40.

Li, Xiaoyu and Alice Robbin, "How China Regulates Online Content: A Policy Evolution Framework." *IADIS International Journal on WWW/Internet*, no.11 (2013): 35-45.

Libicki, Martin. "Cyberwar as a Confidence Game." *Strategic Studies Quarterly*, no.5 (2011): 132-146.

Limaye, Satu. "Minding the Gaps: The Bush Administration and U.S.-Southeast Asia Relations." *Contemporary Southeast Asia*, no. 26 (2004): 73-93.

Lynn, William. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, no: 89 (2010): 97-108.

Miao, Weishan. and Wei Lei, "Policy review: The Cyberspace Administration of China." *Global Media and Communication*, no: 12 (2016): 337-340.

Nye, Joseph. "Nuclear Lessons for Cyber Security?." *Strategic Studies Quarterly*, no: 5 (2011): 18-36.

Rodin, Deborah Norris. "The Cybersecurity Partnership: A Proposal for Cyberthreat Information Sharing Between Contractors and the Federal Government." *Public Contract Law Journal*, no: 44 (2015): 505.

Russo, Kelly and Harvey Rishikof, "Cybersecurity: Executive Orders, Legislation, Cyberattacks, and Hot Topics." *Chapman Law Review* 19, no. 2 (2016): 421-444.

Trachtenberg, David. “Finding the Forest Among the Trees: The Bush Administration’s National Security Policy Successes.” *Comparative Strategy* 23, no. 1 (2004): 1-8.

Valeri, Lorenzo and Michael Knights “Affecting Trust: Terrorism, internet and offensive information warfare.” *Terrorism and Political Violence*, no: 12 (2000): 15-36.

Yang, Guobin. “Chinese Internet? History, Practice, and Globalization.” *Chinese Journal of Communication*, no:5 (2012):49-54.

<u>Official Documents and Reports:</u>

Cyberspace Administration of China, *中华人民共和国网络安全法* [Cybersecurity Law of the People′s Republic of China], http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm (accessed March 12, 2020).

Eric Fisher, Congressional Research Service, *Creating a national framework for cybersecurity: an analysis of issues and options*, 2005, Washington DC: The Library of Congress.

Eric Fisher, Congressional Research Service, *Cybersecurity Issues and Challenges: In Brief*, 2016, Washington DC: Congressional Research Service.

Federal Emergency Management Agency, *Strategic Foresight Initiative*, June 2011.

GAO, *Information security: agencies need to improve cyber incident response practices*, http://www.gao.gov/assets/670/662901.pdf.

Government Accountability Office, *The Department of Homeland Security’s (DHS)*

Critical Infrastructure Protection Cost-Benefit Report, 2009, Washington, DC.

National Communications System, *Supervisory Control and Data Acquisition (SCADA) Systems*, 2004, Washington DC: Office of the Manager National Communications System.

NCSC, *Foreign Economic Espionage in Cyberspace*, (2018):1-15, Washington DC: National Counterintelligence and Security Center.

The Congress, *114TH Congress 1ST Session*. https://www.congress.gov/114/bills/s754/BILLS-114s754es.pdf (accessed March 11, 2020).

The White House, *The Comprehensive National Cybersecurity Initiative*, 2009. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative (accessed Mar 31, 2020).

The White House, *National Security Strategy*, May 2010. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed March 28, 2020).

The White House, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed May 1, 2020).

Newspapers:

Barrett, Devlin. “Chinese national arrested for allegedly using malware linked to OPM hack.” *Washington Post*, August 24, 2017. https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html.

Clark, Grant. “The Great Firewall of China.” *Bloomberg*, November 6, 2018. https://www.bloomberg.com/quicktake/great-firewall-of-china.

Clark, Wesley and Peter Levin, “Securing the Information Highway.” *Foreign Affairs*, November 2009. https://www.foreignaffairs.com/articles/united-states/2009-11-01/securing-information-highway.

Garamone, Jim. “Panetta Spells Out DOD Roles in Cyberspace.” *Department of Defense*, October 11, 2012, http://archive.defense.gov/news/newsarticle.aspx?id=118187.

Gorman, Siobhan. August Cole, and Yochi Dreazen, “Computer Spies Breach Fighter-Jet Project.” *Wall Street Journal*, April 21, 2009. https://www.wsj.com/articles/SB124027491029837401.

Katz, Yaakov. “Stuxnet virus set back Iran’s nuclear program by 2 years.” *Jerusalem Post*, December 15, 2010. https://www.jpost.com/iranian-threat/news/stuxnet-virus-set-back-irans-nuclear-program-by-2-years.

Lu, Xiaomeng. “Scoping Critical Information Infrastructure in China.” *The Diplomat*, May 22, 2018. https://thediplomat.com/2018/05/scoping-critical-information-infrastructure-in-china/.

Lynn, William. “The Pentagon’s Cyberstrategy, One Year Later.” *Foreign Affairs*, Sepember 28, 2011. https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later.

Nakashima, Ellen. “Security firm finds link between China and Anthem hack.” *Washington Post*, February 27, 2015. https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/.

Page, Barnaby. “Pro-Palestinian Hackers Threaten AT&T.” *TechWeb News*, November 11, 2000. http://www.techweb.com/wire/story/TWB20001110S0010.

Ropes & Gray. “An In-Depth Examination of China’s New Cybersecurity Law Part 1: Who Must Comply?.” *Ropes & Gray*, July 7, 2017. https://www.ropesgray.com/en/newsroom/alerts/2017/07/Security-Whos-Regulated-Under-the-New-PRC-Cybersecurity-Law-An-In-Depth-Examination.

Schneier, Bruce. “The Story Behind the Stuxnet Virus.” *Forbes*, Oct 7, 2010. https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#7ab3c4e851e8.

Swaine, Jon. “Georgia: Russia ‘conducting cyber war’.” *The Telegraph*, August 11, 2008. https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

Walt, Stephen. “Is the cyber threat overblown?.” *Foreign Policy*, March 30, 2020. https://foreignpolicy.com/2010/03/30/is-the-cyber-threat-overblown/.

Xinhua News. “Speech at the 2nd World Internet Conference Opening Ceremony.” *Xinhua News*, December 16, 2015. http://news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm.

Online sources:

Cisco. *Cisco 2018 Asia Pacific Security Capabilities Benchmark Study*. https://www.cisco.com/c/m/en_au/products/security/offers/benchmark-reports-2019.html (accessed May 1, 2020).

CNNIC*, Statistical Report on Internet Development in China*, *2017*, The 40th Statistical Report on Internet Development in China, 2017, (1-69), Beijing: CNNIC. https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711387563090220.pdf (accessed May 1, 2020).

Crowell & Moring, *Regulatory Forecast 2016*. https://www.crowell.com/files/Regulatory-Forecast-2016-Crowell-Moring.pdf [http://perma.cc/S2GX-G2NK] (accessed May 2, 2020).

CSIS, *Significant Cyber Incidents*. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (accessed Mar 16, 2020)

DOD, “Department of Defense Strategy for Operating in Cyberspace.” July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed Apr 7, 2020).

Garamone, Jim. “Panetta Spells Out DOD Roles in Cyberspace.” *Department of Defense*, October 11, 2012, http://archive.defense.gov/news/newsarticle.aspx?id=118187 (accessed Mar 26, 2020).

Geers, Kenneth. “Cyberspace and the Changing Nature of Warfare.” 2017. https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf (accessed April 29, 2020).

Goble, Paul. “Russia: Analysis from Washington - a Real Battle on the Virtual Front.” R*adio Free Europe / Radio Liberty*, October 11, 1999. http://www.rferl.org/features/1999/10/F.RU.991011135919.asp. (accessed June 8, 2020).

KPMG China, “MLPS 2.0 Insights and Strategies.” *KPMG China*, May 14, 2017. https://home.kpmg/cn/en/home/insights/2019/05/mlps-insights-strategies.html (accessed June 1, 2020).

Lewis, James. “Cyber War and Competition in the China-U.S. Relationship.” *CSIS*, May 2010. https://www.csis.org/analysis/cyber-war-and-competition-china-us-relationship (accessed March 5, 2020).

Mandiant, “APT1 Exposing One of China’s Cyber Espionage Units.” *FireEye*, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (accessed Mar 30, 2020).

Mi2g. *Evidence Mounts of Pro-Serbian Internet Attack on NATO Countries*. http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/170499.php (accessed March 21, 2020).

PwC, *Managing cyber risks in an interconnected world: key findings from the global state of information security survey 2015*. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (accessed

April 30, 2020).

Ross, Alec. “Want job security? Try online security.” *Wired*, April 25, 2016. https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross (accessed April 5, 2020).

Thomas, Timothy L. “Information Warfare in the Second (1999-Present) Chechen War: Motivator for Military Reform?.” *Foreign Military Studies Office*, 2002. https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/243750 (accessed April 1, 2020).

Xinhua Net, *International Strategy of Cooperation on Cyberspace*. http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm (accessed May 27, 2020).

Books:

Amoretti, Francesco. *Electronic Constitution: Social, Cultural and Political Implications: Social, Cultural, and Political Implications*. Pennsylvania: IGI Global, 2009.

Cheng, Joseph. *China: A New Stage of Development for an Emerging Superpower*. Kowloo: City University of Hong Kong Press, 2012.

Chinese Academy of Cyberspace Studies. *China Internet Development Report 2017*. New York City: Springer, 2018.

Chinese Academy of Cyberspace Studies. *World Internet Development Report 2018*. Berlin: Springer Nature, 2020.

Clancey, Gregory and Hui-Chieh Loy. *Historical Perspectives On East Asian Science,* *Technology and Medicine*. Singapore: World Scientific, 2002.

Dalton, Patricia. *Physical Infrastructure: Challenges and Investment Options for the Nation's Infrastructure*, Washington D.C.: Government Accountability Office, 2008.

Fisher, Eric. Congressional Research Service, *Creating a national framework for cybersecurity: an analysis of issues and options*, Washington D.C.: The Library of Congress, 2005.

Harold, Scott, Martin Libicki, and Astrid Cevallos. *Getting to Yes with China in Cyberspace*. California: RAND Corporation, 2016.

National Research Council. "*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*." Washington, DC: The National Academies Press, 2009.

Tellis, Ashley. *Balancing Without Containment: An American Strategy for Managing China*, Washington D.C.: Carnegie Endowment for International Peace, 2014.

Academic thesis paper:

Jonathan Sims, *Cybersecurity: The Next Threat to National Security*, Master of Military Studies Research Paper, (2011): 1-24.

<u>Korean References:</u>

김관옥[Kim, Kwan Ok], "미중 사이버패권경쟁의 이론적 접근 [The U.S.-China Cyber Hegemony Competitions]." *대한정치학회보* [Korean Journal of Political Science], no. 2 (2015): 231-255.

김상배 [Kim, Sangbae], "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각 [Cybersecurity Strategies of Major Powers in World Politics: From the Comparative Perspective of National Strategies]." *국제 · 지역연구* [International Area Studies]. 26(3). (2017): 67-108.

김상배 [Kim, Sangbae], "사이버 안보와 미중 기술패권 경쟁: 그 진화의 복합지정학 [Cybersecurity and the U.S.-China technology hegemonic competition: The complexity of geopolitics]." *EAI 특별기획논평 시리즈* [East Asia Institute], no. 909 (2019): 1-6.

문가용 [Moon, Ga-yong], "방아쇠부터 클릭까지: 현대 국가들의 치열한 군비 경쟁. [From pulling the trigger to clicking the mouse button: The intense cyber arms race]" *보안뉴스* [Boan News], July 19, 2018, https://www.boannews.com/media/view.asp?idx=71507 (accessed April 17, 2020).

박상돈 [Park, Sangdon], "미국 사이버안보 정보공유법(CISA)의 규범적 의의 [The Normative Meaning of Cybersecurity Information Sharing Act(CISA) of 2015]." *융합보안 논문지* [Convergence security journal], no: 17 (2017): 45-52.

박노형 [Park, Roh-hyung], 정명현 [Chung, Myoung-hyun]. "국제사이버법의 발전: 제 5차 UNGGE활동을 중심으로 [Developments of International Cyber Law: Focusing on the Results of the 5th UN Group of Governmental Experts in Information Security]." 국제법학회논총 [The Korean Journal of International Law], no: 63 (2018) 43-68.

박진형 [Park, Jinhyung], “세계 사이버무기 경쟁시대 개막 [The era of cyber weapon competition begins].” *연합뉴스* [Yonhap News Agency], March 3, 2011, https://www.yna.co.kr/view/AKR20110308207800009 (accessed March 20, 2020).

서의경 [Seo, Eui Kyoung], “중국의 개인정보보호 입법에 관한 연구 – 사이버보안법을 중심으로 [A Study on the Legislation of Personal Information Protection in China - Focusing on the Cyber security law].” 韓國外國語大學校 *中國硏究* [Hankuk University of Foreign Studies Institute of Chinese Studies], no: 72 (2017): 131-152.

송은지 [Song, Eunji], 강원영 [Kang Wonyoung], “미국 오바마 정부 2 기의 사이버보안 강화 정책.” KISA Report. 2014. Available at https://www.kisa.or.kr/public/library/IS_View.jsp?mode=view&p_No=158&b_No=158&d_No=215 (accessed April 2, 2020).

신성호 [Sheen, Seong-Ho], “미 오바마 행정부의 사이버안보 정책과 쟁점 [Obama Administration’s Cyber Security Policy and Challenges].” *국제 · 지역연구* [Institute of International Affairs], no: 25 (2016): 61-96.

임병진 [Lim, Byoungjin], “중국 사이버 안보체계에 관한 연구 [A Study on Chinese Cyber Security Strategy].” (Master’s thesis, Seoul National University, 2017).

안정민 [Ahn, Jungmihn], “미국 사이버안보 정보공유법(Cybersecurity Information Sharing Act)에 대한 소고 [Issues Presented by Cybersecurity Information Sharing Act 2015].” *법학연구* [Journal of Law], no: 28 (2018): 259-282.

조윤영 [Cho, Yunyoung], 정종필 [Chung, Jongpil], “사이버안보(cybersecurity)를 위한 중국의 전략: 국내 정책 변화와 국제사회에서의 경쟁과 협력을 중심으로 [China and Cybersecurity: Responding to Internal and External Challenges].” *21세기 정치학회보* [21st century Political Science Review], no: 26 (2016): 151-177.

조현석 [Cho, Hyun-suk], "미중 사이버 안보 협약 연구 [A Study of the U.S-China Cybersecurity Agreement]." *21세기정치학회* [21st century Political Science Review], 27, no. 2 (2017): 211-228.

Chinese References:

Ji, Guo. "Cyber Should Not Become a New Tool of American Hegemony: Starting from an Explanation of the 'PRISM-gate' Incident [Wangluo buying chengwei Meiguo baquan xin gongju: Cong 'Lingjingmen' shijian shuokai qu]," *Seeking Truth* [Qiu Shi], 2013, no. 15: 57–59.

Jiang Chong, "Cyber: The Invisible New Battlefront [Wangluo: Kanbujian de xin zhanxian]," *Seeking Truth* [Qiu Shi], 2010, no. 13: 53–55.

Yang Jian, "The Nature of the Contextual Contradictions in America's Use of the Phrase ʹCyberspace Global Commons' [Meiguo 'Wangluo kongjian quanqiu gongyu shuo' de yujing maodun jiqi benzhi]," *International Survey* [Guoji guancha], 2013, no. 1: 46–52.

Abstract in Korean
(국문초록)

지난 십 년의 사이버환경은 정치적 목적을 이루기 위한 수단으로써 국가 주도의 사이버공격이 주를 이룬다. 한때 기회주의적 범죄집단에 국한된 사이버공격은 이제 한 국가의 정치적 목적 달성, 사이버 공간에서의 정치적 선전의 중요한 수단으로 이용된다. 이에 따라 사이버공간은 그 귀추가 주목되는 신(新)안보영역으로 급부상하고 있다. 전통적 안보 영역과 비교했을 때 사이버공간의 독특한 특성으로 말미암아 사이버안보 환경을 가늠하는 것은 훨씬 복잡하다. 개방성과 초연결성으로 특징되는 무정형의 사이버 공간에서 역설적이게도 국가는 더욱 국가주의적인 경향을 보인다. 안전한 사이버안보 환경 수립을 위해 글로벌거버넌스 구축의 필요성에 더해 각 국가들이 공동의 이니셔티브를 위해 협력함에도 불구하고 더 우선시되는 주권국가의 이익은 사이버공간이라는 신(新)안보 영역에서의 갈등을 초래할 것이다. 이는 궁극적으로 사이버안보 전망의 구조적 변화를 부추긴다. 사이버공간 하에 한 국가의 정치적 행위가 결국 특수한 목적에 달려있음에 기인해 이 신(新)안보 영역의 이해에 앞서 지정학적 이익관계의 이해가 요구된다.

사이버 역량을 한 국가의 정치적 목적 달성의 수단으로 이용하려는 지난 십 년의 경향은 전통적 안보영역 차원에서 발생하던 일이 사이버공간에 또한 발생할 수 있음을 시사한다. 본 논문은 미국과 중국이 사이버안보 관련 어떠한 정부차원의 조치를 취하는 지 연구함에 목적을 둔다. 양국은 사이버 역량 발전에 국가적 투자를 아끼지 않을 뿐 아니라 동맹국들에게도 협력을 촉구하며 사이버공간이라는 신(新)안보영역에 가장 적극성을 띠는 국가이다. 미국의 2015년 사이버안보법과 중국의 2016년 사이버보안법을 비교 연구해 본 논문은 양국이 국내의 정보 인프라 보호를 위해 어떠한 법적 규제를 마련했는지 살펴보고자 한다. 또한 각국이 사이버공간에서 어떻게 국익을 행사하

며 동시에 범지구적 차원의 사이버안보를 위해 어떠한 협력 매커니즘을 추구하는지 연구한다. 본 논문은 사이버안보를 미·중 경쟁구도의 관점에서 재해석하며 더 나아가 거시적으로 사이버안보를 전망한다는 점에서 현재의 사이버안보 연구에 기여한다.

키워드: 사이버 시대, 미국의 2015년 사이버안보법, 중국의 2016년 사이버보안법, 미국, 중국