China's Cyberspace as a Potential Battlefield:Cyber Sovereignty and Territorilization of Cyberspace

Ji Jen Hwang (黃基禎)

Research Scholar Schar School of Policy and Government George Mason University, USA

Introduction

According to the latest Chinese defense white paper published in July 2019, it points out that "the PLASSF [Strategic Support Force] is a new type of combat force for safeguarding national security and an important driver for the growth of new combat capabilities. It comprises supporting forces for battlefield environment, information, communications, information security, and new technology testing." (PRC, 2019) In other words, the white paper is to regard cyberspace as a potential battleground and to stress how to rule the new battlefield environment via the new combat capability.

In international politics, the relations between sovereignty and territory is vital for a state to claim its sovereign to other states in order to present the legitimacy of its force in the territory. Theoretically, state sovereignty contains four aspects, namely territory, population, authority and recognition. In the

digital age, though Chinese government proposes the notion of its sovereignty in the virtual world cyberspace, as mentioned earlier, it will be lack of legitimacy for China to claims its cyber sovereignty to other international actors in the world politics if the key elements of territoriality have not been identified clearly to enclosure its territory in cyberspace. Therefore, this paper argues that, on the one hand, Chinese government establishes rules of governing cyberspace to claim its so-called cyber sovereignty; on the other hand, an equivalent principle of territory between geographic world and virtual cyberspace has to be identified beforehand to create cyber territoriality for claiming its sovereignty. In order to argue how China territorializes the cyberspace to claim the cyber sovereignty, the paper respectively examines how Chinese government implements cyber laws to support the metaphorical territoriality of cyberspace for China, as well as how cyberspace can be territorialized in general. In conclusion, by arguing an equivalent principle of territoriality between the physical world and the virtual world, the study suggests that cyberspace can be territorialized via three elements of the equivalent principle, namely population, borders, and authority, for conceptualizing China's cyber sovereignty.

Background and purpose of the PRC claiming cyber sovereignty

Cyberspace has expanded into political, economics, and

military fields. Whoever can take command in cyberspace will achieve dominance in the cyberspace.

1. Background of the PRC Claiming cyber sovereignty

(1) Political environment

With the advancement of internet technology, the internet has eliminated the government's dominant position in information dissemination. Cross-border data information has also blurred the boundaries of national sovereignty. In August 19, 2013, PRC President Xi, Jinping spoke at the National Propaganda and Ideology Work Conference. He said, "The Internet has become the main battlefields for the public opinions, it may become a worry in our hearts and minds" (中國數字時代，2013). In addition, on September 27, 2014, in the outbreak of "Occupy Central" in Hong Kong, hacker organization blocked internet services or tampered with websites of 31 websites including Hong Kong Department of Justice, Police Force, radios, and TVB to incite an uprising, which should be vigilant by the Chinese authority (洪京一主編，2015:14-15). Therefore, after the internet becomes a platform for the public to directly participate in the politics, the individualization of the cyberspace power will affect the power structure of the country, society, and individuals. In other words, the free internet space has threatened the legitimacy of the PRC governance, which means that it cannot govern speeches in cyberspace, nor be able to ensure internal security.

(2) Economic environment

Data security cannot be ensured without independent cyber technology. According to Cao, Ruzhong in 2014, since the 1990s, the PRC has been infiltrated by Western countries in the political, economic, and military fields. In particular, the 2013 PRISM of Snowden and the 2014 Microsoft XP shutdown have highlighted the PRC's cyber security has been constrained by others (曹如中、曾瑜、郭華，2014:15-16). In 2014, proxy server for data exchange even had at least 30000 servers in PRC installed with Heartbleed bug[1], affecting social network such as WeChat and Taobao. There are still about 30% of the internet companies in China have failed to enforce their cyber security to protect themselves from the Heartbleed bug (裴毅東，2014:35-37). The integration of cloud database, big data, Internet of Things and other network technologies has turned internet cloud storage data into a target that can be easily attacked by hackers, which posed a huge challenge for the PRC security management system (洪京一主編，2015:17-18). Consequently, facing with the underdeveloped network technology and the lack of awareness toward cyber

[1] Heartbleed Bug was discovered by Google's security team and Finnish cyber security company Codemonicon. The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected and exposed users of e-payment, e-mail, and websites, threatening network devices such as network servers, routers, and radio sharing devices.

security protection in private corporates and the public, free and open cyberspace has threatened PRC's promotion of digital economic development.

(3) Military environment

Whoever can take command in cyberspace will gain initiative on the battlefield. In 2013, 2340 websites of the Chinese government websites were tampered, which was a 34.9% increase compared to the previous year. There were also 2425 government websites that had been implanted with backdoors in the country. The leakage of critical information has threatened the overall national security of the PRC (洪京一主編，2015:109). In addition, according to the "How does the United States Monitoring China- United States Global Monitoring Operation Record" published by the PRC Internet of Things News Research Center in 2014 pointed out that the PRC in monitored by the US National Security Bureau. Their target includes the backbone network of Tsinghua University, the internet room of the telecommunication company Pacnet in the Hong Kong headquarters, even the Tencent chatting software and China Mobile's messenger are all monitoring by the NSA (互聯網新聞研究中心編著，2014:15-19). In addition, since Snowden revealed that the mainland China's internet has been monitoring by the US national security department in 2013, the PRC has adopted a more strict policy to ensure the security of data in their cyberspace. Also, reinforce the development of the internet technology and

military power to interrupt the command and control of US forces with cyber-attack (Greag, Austin, 2015:168). The event of the PRC internet invaded by the United State has shown that a lag in internet technology cannot ensure the security of domestic network. The PRC urges all countries to respect each other's cyber sovereignty are actually trying to solve the problem of internal public opinion on the internet, that countries should not interfere with each other. Strengthening the government's jurisdiction over the virtual economy is also an important means for the PRC to maintain economic development. Furthermore, shaping the cyberspace sovereignty imply that China is claiming the standpoint of their defense forces, which is to prohibit internet hackers to destruct cyber security of other country, in order to prevent the opportunity to provoke can cause cyber conflict.

2. Purpose of the PRC claiming cyber sovereignty

Based on the discussion above, cyber security has threatened the PRC to maintain its national sovereignty, security, and interests. In order to achieve the China Dream and Military Dream, China needed to construct a security cyberspace order.

(1) Increase political influences

Sovereignty means that the state actor has the ruling power inside his territory. According to the "National Cyberspace Security Strategy" at the end of 2016, cyberspace is a new territory for national sovereignty, safeguard national

sovereignty, security, and development in the free and open cyberspace and realize the strategic objective of a building a strong cyber power. At the same time, participate in the formulation of international cyberspace regulation to shape the image of a responsible superpower (中國互聯網路信息中心，2019). In addition, the Chinese government pursues a harmonious and ideal order in the cyberspace, also emphasizes the importance of complying order, as well as personal neutrality and social stability (Frédéric Marte, 2016:57). In the same year, a report published by NATO's Cyber Defense Center on "China and Cyber: Attitudes, Strategies, and Organization" indicated that, in China's political culture, maintaining social order is unquestionably more important than individual privacy. The users of cyberspace, both domestic and foreign citizens within a state's territory, should be controlled by the host state (Mikk Raud, 2016:8-9). Thus, the political purpose of shaping cyber sovereignty is to construct new order in cyberspace in order to shape the international image of the PRC and raise their influence on the international politics.

(2) Raise digital economic competitiveness

With the integration of digital economy, the construction of cyber sovereignty has an advantage in the autonomic development of cyber technology and increase market share. Based on the Communique of the Fifth Plenary Session of the 18th Central Committee of the Chinese Communist Party issued in October 29, 2015, it is necessary to implement the "Internet

+" action plan in order to achieve the strategic goal of becoming a cyber power (中華人民共和國工業和資訊化部，2015). Next year, part six of "The 13th Five-year Plan for Economic and Social Development of The People's Republic of China", The Cyber Economy pointed out that, accelerate the formulation and dissemination of fundamental generic standards and key technical standards for internet can strengthen China's voice in the formulation of international standards (新華網, 2016:46-47). In 2016, Wei, Liang and Wei, Wei's research has confirmed that cyber technology companies supported by the CCP, such as Huawei, Alibaba, and Tencent have increased their market share compare with the past and are influencing the global market (魏亮、魏薇等編著，2016:19). In fact, Jennifer L. Bayuk, former professor of the Stevens Institute of Technology stated, the cyber security of China allows the government to isolate and monitor cyberspace. One of the main purposes is to safeguard its economic development interests. Therefore, the economic purpose of constructing cyber sovereignty is to help foster the competitiveness of its domestic network technology industry and promote integration of digital economy.

(3) Make advantages of the asymmetric operations

Whoever can take command in cyberspace will gain the initiative on the battlefield. According to "The Diversified Employment of China's Armed Forces" issued by the PRC State Council in 2013, China has to maintain strategic

superiorities in cyberspace in order to win local wars under the conditions of informationization (中華人民共和國國務院新聞辦公室，2013年). In addition to avoid the virtual Tiananmen event from happening, the cyber strategic goal of the Chinese government should also include the combat readiness of winning a digitized global war (Frédéric Marte, 2016:62-63). Moreover, the cyber forces of the Chinese People's Liberation Army (PLA) is attached to the cyber operation department under the former General Staff Headquarters, which indicate the attempt of the Chinese government to use cyber forces to gain advantage in asymmetric operation and realize the status of regional Hegemon (Francis C. Domingo, 2016:165). Therefore, before cyber warfare is clearly defined by the international community, the military purpose of shaping cyber sovereignty can help CCP monitoring data flow, improving its cyber defense capabilities, and shaping the legitimacy of counterattacks of the cyber forces.

The purpose of the PRC shaping cyber sovereignty in summary: Politically, maintain internal political attitudes through the examination of internet. Externally, construct new order in the cyberspace to increase political influences. Economically, foster domestic internet technology industry to occupy the market and strengthen international competitiveness. Militarily, required domestic and foreign network operators to set up a data center in China and turn over source code of the program based on the "Network Security

Law", in order to eliminate the risk of the implantation of computer viruses from using operation system developed by other countries; in addition, increased the deterrent ability of cyber warfare. In short, the purpose of the PRC declaring its cyber sovereignty is to construct a cyberspace that meets its core interests, and support the promotion of digital economic integration of the "One Belt, One Road," ultimately, fulfill the strategic goal of the China Dream and Military Dream.

Assessing of the scope of the PRC's construction of cyberspace borders

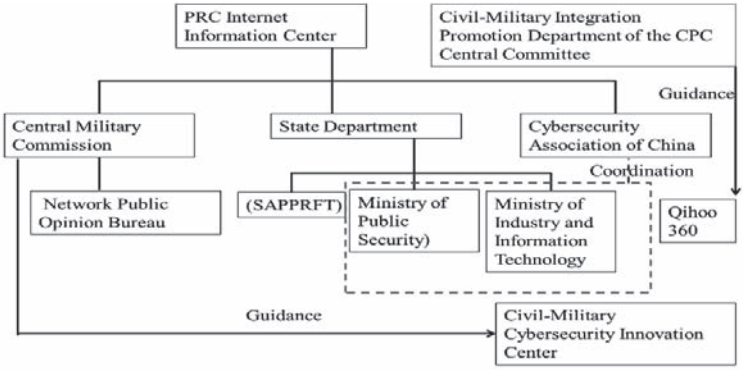
Factors to be considered when constructing the territorialization in the free and open cyberspace, internally, is the organization function and internet technology within the administration; externally, is the current US-led cyberspace management order.

1. Establish a cyberspace security department

A department with unity of direction and responsibility of duty must be established within an organization to reinforce cyber security defense. With the expansion of the impact of cyberspace, to ensure security of data, departments that deals with internet network reconnaissance, tracking, processing, responding, should be integrated. In February 27, 2014, the Chinese Communist Party established the "Central Leading Group for Cybersecurity and Informatization" and was chaired by President Xi Jinping. The department is responsible for overall planning and coordinating issues of cyber security and

in all the aspects (新華網，2014). In addition, the China Internet Information Center coordinates with the Ministry of Industry and Information Technology and the Ministry of Public Security (惠志斌，2015:146). Furthermore, the iBooks stores of the US Apple computer ware banned by the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) of the PRC (Paul, Mozur and Jane, Perlez, 2016). Moreover, the Chinese People's Liberation Army established the "Chinese Military Network Report Platform" under the guidance of the Central Military Commission network public opinion bureau in November 19, 2017 in order to safeguarding the internal cyber security. The purpose of this platform include investigate the falsifying military news headlines, publishing information that is harmful or insulting the military, attacking the leadership of the Communist Party, or revealing a soldier's personal identity (李景璿、陳泰偉，2017).

Figure 1. Organization of the cyberspace borders constructing by the CCP



With the increase in the population on the internet, PRC established its first “Cybersecurity Association of China” on March 26, 2016 to mobilize the society to participate in the maintenance of cyber security. The organizations include the officials of the Ministry of Civil Affairs, the Ministry of Industry and Information Technology, the Ministry of Public Security, Internet Society of China, Qihoo 360, and the Antian Technology (中國互聯網路信息中心，2016). In addition, at the end of December, 2017, following the guidance of the Civil-Military Integration Promotion Department of the CPC Central Committee and the relevant departments of the PLA, Qihoo 360 established the Civil-Military Cybersecurity Innovation Center. The goal of the Center is to carry out the strategy of cyber power (張新、楊利程，2017). Therefore, department maintaining the PRC cyberspace security is led by the “Central Leading Group for Cybersecurity and Informatization,” the Ministry of Industry and Information Technology, the Ministry of Public Security, the State Administration of Press, Publication, Radio, Film and Television, and the civilian “Cybersecurity Association of China.” In other words, China’s cyber sovereignty policy has integrated in the China Internet Information Center and become the core task of various departments. The borders of cyberspace are also constructed in the execution of the departments (See figure 1. Organization of the cyberspace borders constructing by the CCP).

Resources: Based on the official "China Internet Information Center," PLA Report and resources from various scholars. Cited from 惠志彬(2013)；中華人民共和國國家互聯網網路信息辦公室(2016)；張新、楊利程(2017)；李景璿、陳泰偉(2017)。

2. The ability to control cyberspace borders

The cyberspace is constructed by the users of internet through the critical network infrastructure in the country and the internet agreement. Therefore, to access the constructed scope of cyberspace boundaries depends on whether it is within the jurisdiction of the government.

(1) Internet user jurisdiction

National cyber security cannot be secure without governing the flow of data. According to Article 1 of the China's Cybersecurity Law, for the purpose of maintaining network security, safeguarding the cyber space sovereignty, national security and public interests, protecting the legal rights and interests of citizens, corporations and other organizations, and promoting the healthy development of information technology in the economic and social (中國人大網，2016). In January of the following year, the Ministry of Industry and Information Technology of the PRC issued a "Notice on Cleaning Up and Regulating the Internet Access Service Market" to requests state-owned telecommunication providers including China Mobile, China Unicom, and China Telecom to ban the individual users from applying for VPN. Domestic

enterprises have to register for related services before they can use the dedicated lines to connect to the international network (中央社通訊社，2017). On August 25, 2017, the Cyberspace Administration of China issued the Administrative Provisions on Online Comment Threads Services, requiring users to follow the principle of 'foreground voluntary name, background real name' when registering accounts. Network operators cannot provide internet services without verifying identity of the user (中華人民共和國國家網信辦公室，2017). Internet users and operators are under scrutiny, which means the cyber borders are being drawn.

Look back at history, the Chinese Communist Party has already set up a monitoring system to enforce cyber security. The "China National Firewall" or "Great Firewall" (GFW), that automatically filtered statement that are harmful to the government and block the connection of certain IPs, such as Facebook, YouTube, and Twitter (過子庸，2011:100). In addition, the Chinese government used cyber security as justification to force foreign companies, Microsoft for example, to turn over source code that allows the government to monito internet users (呂晶華、成高帥譯，2011:43-44). In May 2017, Russia also banned We Chat, the social media app developed by Tencent, which is closely related to the CCP (高紫檀，2017). At the end of November of the same year, India also demanded troops that stationing in the China-India border to deleted We Chat and Wei Bo from their smart phones. They

believed that the software developed by the CCP may have been installed with spyware or other malicious programs (Manu Pubby, Manu Pubby).

In order to control the data flow of domestic user, the CCP has already established a set of government-to-people data monitoring rights. After the issuing of the Cyber Security Law in 2016, Chinese government will gain more jurisdictions over domestic users to check and block individual's access to the internet. The law also requires domestic and foreign cyber technology companies to turn over their program source code and build data centers when then enter the Chinese market. Therefore, the cyber sovereignty shaped by the CCP has extended its control beyond the national border, which means that the CCP intelligence agencies can use the source code provided by the internet companies to monitor users whether or not the user is in the country.

(2) Critical cyber security protection in the nation

It is important to ensure the security of domestic critical infrastructure such as information and communications in order to prevent form cyberattacks. The CCP cyberspace structure is divided into core and regional layers. The core layer is composed of the core nodes of 8 cities, including Beijing, Shanghai, Guangzhou, Shenyang, Nanjing, Wuhan, Chengdu, and Xi'an. The function is to connect the international internet as a network exchange between large-scale layers. There is a non-fully mesh structure in between, in which the core nodes

of Beijing, Shanghai, and Guangzhou each has an international export network proxy server, responsible for connecting with the international network. The large-scale layer includes 31 provincial capitals within China that constructed into 8 large-scale networks based on their core layers. Large-scale networks provide information exchange within the layer and access to the internal network Chinanet (惠志斌，2015:14). In addition, in order to prevent the cyberspace from being monitored by other country, China is planning on deploy a 2000 km of Quantum Secure Communication backbone network for the backbone links between Beijing and Shanghai core layers (洪京一主編，2015:68-69). Furthermore, the Quantum Secure Communication backbone network, the "Beijing-Shanghai Trunk Line" (712km) was opened on November 21, 2016 from Hefei to Shanghai, to provide secure communication services for financial and governmental industries in the Yangtze River Delta region (徐海濤，2016). Therefore, through the deployment of internal and external internet proxy servers (international exports: Beijing, Shanghai, Guangzhou), and quantum secure communication backbone network, the CCP cyberspace border has been shaped contrasted with land-power.

In 2015, first Chinese made firewall (HT706-2000 gigabit) was developed by No. 706 Institute of CASIC Second Academy and has passed the military information security evaluation certification. The firewall will be deployed between

the internal network of enterprises and public network to ensure the cyber security of the internal network (中國芯防火牆國內率先通過認證，2015:109). In addition, according to the Cyber Security Law of 2016, government should take the initiative to monitor cyber security threats from home and abroad in order to protect critical information and communication facilities and maintain security and order within the cyberspace (中國人大網，2016). Furthermore, based on the report of the Rand Corporation in 2018, the information operational system of the CCP cyberspace has become an internal network isolated from the international internet, which can prevent the breakthrough of cyberspace boundary, its capability including anti-virus attack, anti-hacker attack, and network emergency recovery (Jeffrey Engstrom, 2018, pp115-116). Therefore, the issue of Cyber Security Law and the advancement of cyber technology has enable the formation of an internal network within China to be isolated from the global network.

(3) Cyber Agreement

Cyberspace has no borders; therefore, country's that dominate the formulation of cyber agreements and own the advanced technology will be able to take command in cyberspace. In November 26, 2017, Chinese Communist Party Central Committee and the State Council jointly issued an Action Plan for Promoting Large-scale Deployment of Internet Protocol Version 6 (IPv6). According to the Plan, website

system of government above provincial-level and central enterprises, and commercial websites ranking the first 50 in terms of the number of users in China and their application have to fully adopt IPv6 by the end of 2018; and by the end of 2025, all network in China should fully support IPv6 (State Council, 2017). Consequently, the IPv6 network protocol actively developed by the CCP will enable every information device that can connect to the Internet in China to have and IP address. This also means that the Chinese government is more capable of tracking data with a network protocol that is different from the rest of the world. Overall, the concept of cyber sovereignty is shaped by the CCP with support of its policies and network technology to draw the cyberspace borders. In particular, since the issue of Cyber Security Law in 2016, Chinese government can demand network operator within China to turn over the source code of their product, together with the self-developed Great Firewall, monitoring internet users more strictly. With the Quantum Secure Communication backbone network and network protocol IPv6 led by the government, China can also construct a barrier to prevent attack in the cyberspace. In other words, the cyber sovereignty shaped by China, with the basis of cyberspace border, divided into physical borders that is critical infrastructure such as information and communication, and the virtual border, which will expand with the national defense force and system developed by the CCP civilian network

technology used by other countries (see Figure 2. the cyberspace borders of cyber sovereignty shaped by the CCP).

3. Challenge of the CCP Cyberspace Construction

The claiming of cyber sovereignty will challenge the US cyber strategic goal of promoting democratic and free universal values.

(1) Freedom and democracy are the soft powers of the United States

The democratic peace theory has always been the best argument for the United States to maintain the international system. State actors have been using internet social media to obtain domestic public support and influence international public opinions to have an effect on the development of other countries. In January 2010, former US Secretary of State Hillary Clinton publicly stated that the United States is committed to help promoting Internet freedom. She also encouraged countries to respect the global public domain and that governments should not hinder people's freedom to use the Internet and access websites (Adam Thierer, 2010). In addition, in January 6, 2018, US Secretary of State Steve Goldstein urged the Iranian government to stop cutting off domestic internet communications and blocking widely used social media sites like Instagram in order to stop anti-government activities, or the United States has an obligation not to stand by (Danika Fear, 2018). Furthermore, CCP's promotion of cyber sovereignty would be challenged the most by unilateralism and

hegemony of the international cyberspace (王春暉，2016:14). Therefore, the cyber sovereignty claimed by the CCP to try to construct a cyberspace isolated from the world has affected the international peace shaped by the United States. In other world, the first challenge for China to shape cyber sovereignty is to preserve reputation of being a superpower and avoid being caught up in what the Western countries regard as the "China threat theory."

(2) Violate commercial interests in U.S. cyberspace

The free and open cyberspace will stimulate global economic and trade development. On the contrary, shaping the network border unilaterally will discourage global economic and trade exchange. In 2013, Kris E. Barcomb identified seven strategic points of concentration in cyberspace for the United States, including operating system, search engines, physical communications infrastructure, cloud computing, governance forums, cryptography, and Internet Protocol version 6 (IPv6), to maintain the cyber security of US government, corporations, and individuals. In addition, take the advantage of these seven strategic points of concentration in cyberspace to facilitate the growth of American private enterprise in cyberspace and thereby improve the US leadership in this domain (Kris E. Barcomb, 2013:80-83). It is also worth noting that the CCP systematically subsidize the development of its network, telecommunication industries, and private equipment suppliers with the purpose of improving economic development and

political influences. For example, Facebook and Twitter were banned from entering the Chinese market in 2009, which was slightly earlier than the launch of Sina Weibo (Frédéric Marte, 2016:60). Therefore, cyberspace dominance has become the strategic goal of both China and the United States. However, the cyber sovereignty shaped by CCP has affected the cost of foreign operators to enter Chinese market which has impacted on the interests of American private companies. As a result, the second challenge will be the competitiveness of the Chinese network technology, and that the United States will counterattack based on its own interests. For instance, the United States put a restriction on Chinese private communication company such as Huawei in 2018, which is detrimental for the selling of Chinese internet products to the world market.

(3) Impact on the US Defense Strategy Objectives and Security

The Internet was created when the US Department of Defense began to enforce the command and control links. As a result, cyberspace dominance has always been the top priority of the US strategic objectives. In 2011, the White House published the International Strategy for Cyberspace and indicated that the US will continue to ensure the openness and interoperability of cyberspace so all can benefit from it, while opposing efforts to splinter this network into national intranets (The White House, 2011). In addition, according to Susan

Shirk's research in 2017, the United States should continue to maintain close relationships with Asian allies in cyberspace policy, but take a tough stance against the CCP to defend the interest of US in cyberspace (Susan Shirk, 2017:15). Therefore, from the military perspective, the cyberspace borders constructed by the CCP have hindered the strategic intent of the United States to ensure its safety and interest. The third challenge for China is in the cyberspace defense system, which cannot surpass the United States in cyber technology, and the cyber force cannot defend its borders, thus, the US cyber force can act freely keeping with its strategic intent.

A national defense cyber force is necessary in defending cyberspace security and interests. To ensure the security of cyberspace between the government and businesses, government needed to construct cyber forces to isolate their information in the physical networks (Jason Andress, Steve winterfeld, 2014:35-36). Furthermore, according to the US congressional report in 2015, even though the Tallinn Manual has set out rules governing cyber conflict addressing international law and the law of armed conflict, but when cyber technology failed to identify the cyber attacker, the motives of the individual, or whether the cyberterrorists are state-sponsored who engage to pursue their military objectives, the Tallinn Manual can only provide the rules of engagement in cyber warfare but not constrain international cyber behavior (Catherine A. Theohary, John W. Rollins, 2015:5). Therefore,

since the CCP cyber technology and cyber forces are still lag behind the US, the cyberspace defense great wall will not be able to achieve the deterrence strategy.

Overall, the United State and China are both constructing cyber sovereignty to ensure their security and interests. However, the United States stand for the freedom of Internet and advocate its democratic and freedom values through the free and open cyberspace to influence the international system, taking the advantage of network technology to bring more profits to its private network technology enterprises. In addition, the US national security department uses the advantage of network technology to monitor and control global intelligence to ensure national interests and security. On the other hand, although the cyber technology of the CCP cannot compete with the US, the cyber policy led by government, the development of military and civilian technology, and the largest internet population of about 731 million has isolated CCP's cyberspace from the rest of the world.

Table 2. The analysis of the cyber sovereignty construction of CCP and the US

	Chinese Communist Party	United States Government
Policy Standpoint	Cyber Sovereignty	Freedom of Cyberspace
Purpose	Break the current order of cyberspace and construct a cyberspace that can be managed by the Chinese government to maintain PRC interests and security.	Keep current order of cyberspace and construct a US dominated cyberspace to maintain US interests and security.
Objectives	Physical domain of the cyberspace such as critical infrastructure, internet agreement, or corporate databases, and personal data (personal speeches on the social media), are subject to jurisdiction (review and delete content of online	Physical domain of cyberspace is subject to jurisdiction, but personal monitoring must be approved by the court (without content review). In addition, global users can be monitored to deter cyberterrorism.

	media).	
Method	Claiming cyber sovereignty and advocate a mutual respect cyberspace culture. Extend national sovereignty to cyberspace through international cooperation.	Advocate the freedom of cyberspace and leading international cooperation. Extend national sovereignty to cyberspace through military forces projections.
Technique	Self-developed network technology.	Export network technology to the world.
Network Agreement	Fully adopted the IPv6 network protocol in China by 2025.	Control the allocation of cyber resources.

Conceptualizing 'territoriality' of cyberspace

Traditionally a state is protected inside a geographic territory surrounded by physical borders – natural barriers such as rivers, oceans, straits, mountains, and special terrain. These boundaries also distinguish the state's territory and determine its territoriality. In general territory in the modern state system was protected by borders lined with fortresses and fortifications

to form a 'hard shell' (Herz, 1962).[2] However, in the atomic age, destructive weapons perhaps changed such territorial thinking as nuclear power shattered all previous conceptions. This may well occur again as a result of cyber warfare in the digital age, since the geographical protection of a state is far removed from cyberspace. For instance, research points out that any fresh meat passing the physical border into a country will be inspected, but a malicious attack via cyberspace could be transmitted unchecked across 20 borders by the click of just one button (Nykodym and Taylor, 2004). As the virtual 'territory' of cyberspace is shaped differently to the physical world, traditional borders cannot ensure state security against cyber attacks; instead, each state needs to formulate new strategic approaches to guard its relevant surroundings. However, cyberspace is also a space like land, sea and air. States or non-state actors can interact and communicate with one another through these spaces, and share the resources arising from them. As David Fahrenkrug (2008:135) argues, strategists often make the big mistake of erroneously focusing just on information, and not on cyberspace itself – the platform

[2] In addition, Herz also provides an example from Mencius, an ancient Chinese philosopher, to reflect the condition of territorial security. Mencius provided guidance for the governor of a small state about a thousand years ago, advising: 'Dig deeper your moats; build higher your walls; guard them along with your people.' (Herz, 1962:107)

which bears the information. Fahrenkrug provides the example of sea as a modern line of communication for states. It is far more important to securely maintain this line of communication than to protect the goods transported through it. He goes on to extrapolate that instead of protecting the information itself, securing cyberspace as a domain, where information is stored, transferred, and modified via a computer system, should be the aim of theory and strategy. (Fahrenkrug, 2008:141) Unfortunately, according to Hansen (2008:43), although the US Joint Chiefs of Staff approved the definition of cyberspace and recognized that it was a potential battleground as early as October 2006, military doctrines relating to cyber warfare still remain uncertain.

What's more, conceptual boundaries, such as proxy servers acting as functional borders, are essential in cyberspace for actors to recognize respective ownership, as actors may include states, non-state organizations, private companies and even individuals. In other words, it could be constructive to establish a conceptual 'territory' for each actor in cyberspace, so that the actors can demarcate their zone of responsibility and proclaim their 'authority', which may imply equivalence to 'sovereignty'. Servers, routers and network protocols can be employed technically as functional borders to form this corresponding 'territory', as well as protecting against attacks in cyberspace. This research argues that cyberspace could be conceptually territorialized by the Domain Name System,

TCP/IP, and functional borders, creating a new virtual realm. This new conceptualized territory also leads to a virtual territoriality[3], which could be dubbed *cyber-territoriality*, where in addition to states, non-state organizations and private companies are also actors in cyberspace. In other words, it is not necessary that owners of cyber-territoriality be only states, but can also be private actors who have the authority of managing the 'functional borders' created by IP addresses and the DNS.

Moreover, definitions of territory[4] seem to assume that

---

[3] Territoriality is a term associated with nonverbal communication, referring to how people use space to communicate ownership/occupancy of areas and possessions. (Beebe, Beebe, and Redmond, 2008:209)

[4] The word 'territory' is defined in Merriam-Webster's Collegiate Online Dictionary as:

1. a: a geographical area belonging to or under the jurisdiction of a governmental authority.
   b: an administrative subdivision of a country. c: a geographical area (as a colonial possession) dependent on an external government but having some degree of autonomy.
2. a: an indeterminate geographical area; b: a field of knowledge or interest.
3. a: an assigned area; especially: one in which a sales representative or distributor operates; b: an area often including a nesting or den site and

territory exists innately, and in a general sense involves not merely an actual and already existing geographical area, but the relation of this area to either humans or animals. Wolfgang Kleinwächter (2000) put forward the concept of 'territory of cyberspace,' conceptually constructed upon the Domain Name System and IP addresses, but he did not go so far as to explain the potential territorialization of cyberspace. As Robert Sack argues, 'Territories are socially constructed forms of spatial relations and their effects depend on who is controlling whom and for what purpose,' and 'Territoriality in humans is best understood as a spatial strategy to affect, influence, or control resources and people, by controlling area; and, as a strategy, territoriality can be turned on and off.' (Sack, 1986:216) As a result, a territory is not merely a geographical space, but also a conceptual space such as cyberspace. These discourses, proposed from the field of philosophy, construct the argument that territory is not confined to a geographical area; it can also be something abstract: a concept, rather than a geographical zone. In other words, though the word 'territory' is derived from geography, the concept of territory can also be conceptually regarded as a sphere of autonomy in accordance with its ownership. As discussed in depth in Section 2.1, cyberspace, constructed of interconnected computer networks,

variable foraging range that is occupied and defended by an animal or group of animals.

provides an infrastructure for information exchange and communications based on the Domain Name System (DNS) and the mapping of IP addresses. This indispensable information platform is structured by combining a large amount of physical hardware, such as computers, servers, routers, converts, and cables, with conceptual interactions, such as information exchange and communications. The authority to control these individual physical systems and to access their information potentially constitutes a virtual territory of cyberspace, leading to the 'territorialisation' of cyberspace. As Ian Buchanan and Adrian Parr (2006:194) examine, the concept of the virtual territory has already been applied to cyberspace in the work of Deleuze and Guattari[5].

The main achievement of the Domain Name System is to create a conceptual space which regulates dispersed IP addresses into a well-organised and strictly individual hierarchy: a name space under a certain domain. However, if

[5] In the book, *Thousand Plateaus*, 'the territory is the product of a territorialization of milieus and rhythms…A territory borrows from all the milieus; it bites into them, seizes them bodily…It is built from aspects or portions of milieu…There is a territory precisely when milieu components cease to be directional, becoming dimensional instead, when they cease to be functional to become expressive…What defines the territory is the emergence of matters of expression.' (Deleuze and Guattari, 1988:314-315)

the DNS were temporarily ignored, only the relation between assigned IP addresses and their connected hosts would be considered. It could be judged that the geographic mapping between the space constructed by IP addresses and the geographic space constructed by these host computers becomes meaningless, since there is no rational or regular relation between them. In other words, without the DNS, IP addresses would just be a series of numbers, and their allocation would be arbitrary, especially in terms of geographic distribution. Therefore, if the DNS were somehow removed and then brought back, the map of cyberspace would be totally different. Under this new DNS framework, cyberspace would have a meaningful and hierarchical structure; thus, in contrast to the chaotic image of cyberspace established by IP addresses only, the DNS would create a well-defined construction. Cyberspace would be reconstructed as a hierarchical realm by the DNS and IP address system. In this hypothetical example, the Domain Name System (DNS) would not merely rebuild the system ruptured by use of IP addresses alone, but also deconstruct itself from its technical field and then reconstruct itself. In addition, this issue cannot be described only from a technical point of view; it must also be considered from social and cultural dimensions, since the difference between 'dajkjw 23ds.org' and 'cybersecurity.org' or 'chinese-web.org' cannot be answered in terms of technical orientation, as their functions are all the same from the DNS's point of view.

Certainly, technology causes some structural limitation, but the motivation of matching domain names with popular terms used in real life or special meanings goes far beyond technology itself. The DNS reconstructs the relationship between distributed IP addresses and well-structured domain name spaces to establish a virtual territory of cyberspace, which also obtains symbolic values and names which can only be noticed in the social environment in which they are used. In addition, each computer has a name assigned by an Internet Service Provider (ISP) when connecting to the internet to identify its position in the whole hierarchical name space. In the real world, it is possible that two people may have exactly the same names, which is not a problem as people are identifiable through other means. However, this is impossible in the virtual territoriality of cyberspace even if two machines are identical. The name space is exclusively at any time under the principle of universal response, according to which the same query always gets the same answer no matter where it was asked or what server name was required. Unlike in real life where one's name and space or location are separate, under the Domain Name System, a name represents space and location. There is no possibility for the identical, and that creates an extremely rigid territoriality. In the next chapter this research will generate a theoretical tool, equivalent to the principles of the territorial state system, in order to identify whether or not the virtual territoriality of cyberspace is being intruded upon.

Conclusion

Cyberspace is recognized as the 5th domain following land, sea, air, and space. As cyber security threatens the global digital economy, national sovereignty, and security development, the localization of data construction has become an important measure for countries around the world to ensure the security and benefits of cyberspace. With the passing of bills for data localization has passed in countries around the world, cyber sovereignty has become a new type of sovereignty that state actors must face and claim. In short, cyber sovereignty will play a more important role in the future international system than before. Following the trend, the Information and Communication Security Management Act of the ROC is currently in the legislative review stage. Concept of shaping cyber sovereignty and whether the object and scope of jurisdiction will conflict with issues such as human rights and intellectual property rights remain arguable. Even though data localization has become an important measure for countries to ensure cyber security, the cyber territorialization, shaped by an authoritarian regime like the CCP, may still have impact on regional security. From 2011 to 2016, the cyber sovereignty declared by the CCP has turned into the construction of new order in the cyberspace from ensuring the social security at the beginning. The enforcement of internal political ideology review remains the same, while the construction of cyber sovereignty can help foster domestic network technology and

indirectly enforce the security protection capabilities. In addition, the monitoring of data flow by military forces can safeguard cyberspace and interests. The result: Politically, become a political tool to suppress domestic political dissent. Economically, the unfair economic and trade competition will have impact on the development of free trade and economy. Militarily, monitor information of other countries with the source code of the products and support the soft and hard military power to deter enemy in cyberspace. Overall, China can fulfill its China Dream and Military Dream by declaring cyber sovereignty and will have impact on regional security.

The free and democratic cyberspace dominated by the United States has been impacted by the cyberspace territory shaped by the CCP. In addition, the cost of private companies entering the market in China has increased and affects the strategic interests of the United States. The United States is bound to take countermeasures in order to safeguard its national interests. For example, China's Huawei communication corporation was not allowed to enter the US market in 2018. Therefore, whether the CCP will change its internet policy due to pressure from the US or use diplomatic and economic measures to enforce the influences in cyberspace will be worthy of a follow-up observation.