THE CHINESE MODEL OF CYBER SOVEREIGNTY: MAIN PRINCIPLES AND IMPLEMENTATIONS*

Enescan LORCİ**

Makale Geliş Tarihi/Received: 26/10/2021
Makale Kabul Tarihi/Accepted: 21/12/2021
Makale Yayın Tarihi/Published: 31/12/2021
Atıf için/To cite: Lorci, E. (2021). The Chinese Model of Cyber Sovereignty: Main Principles and Implementations. *Uluslararası İlişkiler Çalışmaları Dergisi, 1*(2), 149-163.

Abstract: The invention of the internet by a group of engineers in the United States of America in the late 1990s caused enormous changes in people's lives and brought some major debates in the international arena. Undoubtedly, one of the most important of these debates was what should be the scope and limits of states' sovereignty in cyberspace that emerged with the use of the internet. This issue caused a serious disagreement between the US with a techno-optimistic approach, and authoritarian states such as China, Russia, and Iran. While the countries adopting the techno-optimistic view opposed the hegemony of the states in cyberspace, authoritarian states including China argued that cyberspace is a reflection of the physical territory of the state and that states should have full sovereignty in cyberspace. In this context, this article explains China's position in this debate through the explanation of the existence, development, and implementation of China's concept of cyber sovereignty**.**
Keywords: China, The United States, Internet, Cyberspace, Cyber Sovereignty

ÇİN'İN SİBER EGEMENLİK MODELİ: TEMEL İLKELER VE UYGULAMALAR

Özet: 1990lı yılların sonlarına doğru internetin Amerika Birleşik Devletleri'nde bir grup mühendis tarafından icat edilmesi insanların yaşamlarında büyük değişiklere neden olduğu gibi bazı büyük uluslararası tartışmaları da beraberinde getirdi. Şüphesiz bu tartışmaların en önemlilerinden bir tanesi internetin kullanımıyla birlikte ortaya çıkan siber alanda devletlerin egemenliklerin kapsam ve sınırlarının ne olacağı konusuydu. Bu mesele konuya tekno-iyimser bir yaklaşıkla bakan ABD ve Batı devleriyle Çin, Rusya, İran gibi otoriter devletler arasında ciddi bir fikir ayrılığına neden oldu. Tekno-iyimser görüşü benimseyen ülkeler, devletlerin siber alanda hegemonya sahibi olmasına karşı çıkarken Çin'in de içinde bulunduğu otoriter devletler siber alanın devletin fiziksel sınırlarının bir yansıması olduğu ve devletlerin siber alanda tam egemenliğe sahip olması gerektiğini savundular. Bu bağlamda bu makale Çin'in bu tartışmadaki konumunu, Çin'in siber egemenliği kavramının oluşum süreci, gelişimini ve uygulamaları üzerinden açıklamaktadır.
Anahtar Kelimeler: Çin, ABD, İnternet, Siber Alan, Siber Egemenlik

* This article was produced from the master's thesis that was completed on 29.06.2021 titled "Chinese Cyber Sovereignty in Sub-Saharan Africa: The Perspective of Digital Colonialism".

** PhD Student, National Sun Yat-sen University, Institute of China and Asia-Pacific Studies, enescanlorci@gmail.nsysu.edu.tw

https://orcid.org/0000-0003-0111-6331

Introduction

The lexical meaning of technology is the branch of knowledge that deals with the creation and use of technical means and their relationship with life, society, and the environment, drawing upon such subjects as industrial arts, engineering, applied science, and pure science. The development of technology dates back to ancient times, even back to the making of the first simple tools. After the Middle Ages, the modern technology era started, especially with the “Industrial Revolution”. In the 20th century, the development of technology reached in an unprecedented speed and began to change the living standards and styles of people. With the mass production in automobile production, for instance, in the 1900s, automobile prices decreased and the number of people who own cars in industrial societies increased accordingly. In this way, traveling from one city to another or from rural areas to urban areas became easier. In addition to this, thanks to development of electronic technologies first transatlantic radio message were sent and few years later television invented as a new mean of communication. Finally, with use of modern computer after Second World War the internet was invented in United States by group of engineers.

The rapid development of the internet and related technologies affected all aspects of people’s life. Besides, noticeable changes in people's lives, the rapid development of the Internet and related technologies also brought some new debates in international politics. Undoubtedly, one of the most important of these discussions was what should be the roles, responsibilities, and authorities of states in the cyberspace that emerged with the internet. In other words, what should be the scope and limitations of the cyber sovereignty of the states? Although, many different definitions of sovereignty could be made, this article will focus on the concept of territorial sovereignty, as it explores state sovereignty in cyberspace. Territorial sovereignty can be explained as a "state exercises principal means of authority within a given territory" (Goldsmith, 1998). Despite the fact that "given territory" is always one of the fundamental elements while talking about sovereignty, for some scholars because of the architectural design and the definition of the internet, it cannot be territorialized (Goldsmith, 1998).

According to the techno-optimistic view that emerged especially in the USA after the invention of the Internet, the Internet is a communication tool that was invented on libertarian foundations with the main purpose to increase communication between individuals and societies(Creemers, 2020). Thus, these techno-optimists argued that the internet cannot correlate with the physical location because cyberspace is a separate place removed from our world. Hence, states do not have sovereignty in cyberspace. Although this techno-optimistic view, supported by many thanks to the moderate atmosphere that emerged in the international arena after the cold war, it did not take long for opposing ideas to emerge. The main point defended by those oppositions of techno-optimistic view was although the internet does not necessarily correlate with physical location due to its architecture, the basic structural elements that create the internet such as software and hardware are located within the borders of a certain state, and therefore, the activities carried out in the cyberspace should not be contrary to the regulations of the current state (Creemers, 2020). Otherwise, every individual will be responsible for their activities towards governments in cyberspace (Goldsmith, 1998).

In the next period, the states also initiated to express their opinions about how the state's sovereignty in cyberspace should operate. In the United States where the internet was invented and used with the liberal foundations for the first time, and Western states that deem value issues such as democracy and human rights adopted a view close to the techno-optimists and argued that states cannot be a hegemon in the cyberspace (Schia & Gjesvik, 2017). On the other hand, authoritarian states such as China, Russia, and Iran see cyberspace as a reflection of the physical territory of the state and underlined that all individuals and institutions operating in cyberspace are obliged to comply with the rules of that state. (Schia & Gjesvik, 2017).

When the development of the internet and cyberspace was analyzed in China, many Western and American scholars argued that the spread of the internet in China would enable the Chinese people to reach information outside of China and learn more about the Western democracies. Thus, the people would demand more freedom and democracy which would, later, lead to the collapse of the communist party. However, contrary to what scholars thought, the spread of the Internet in China did not lead to the collapse of the Communist party, but rather played a crucial role in increasing the control and legitimacy of the party over the Chinese people. The main reason why the spread of the Internet in China did not cause the collapse of the communist party but rather increased its legitimacy was the Chinese government, from the very beginning, saw the Internet not as a tool to increase freedoms and communication, but as a must-have tool to achieve its economic goals (Jiang, 2010). The main purpose of the Chinese government was the reach economic development and stability that the internet would lead to but at the same time avoid any possible harm that would exist with the adoption of the internet. Thus, the Chinese government, from the early beginning, hold the internet under control with many legislative and administrative regulations. Moreover, the Chinese government transformed the internet into a tool for controlling Chinese society (Jiang, 2010). This mechanism, with Xi Jinping's coming to office, started to call Chinese cyber sovereignty. This movement, undoubtedly, is seen as the Chinese government's way of legitimizing its unethical actions in cyberspace.

In this context, the main purpose of this article is to explain what is the concept of Chinese Cyber sovereignty, its development process, and its implementations in China.

1. Sovereignty in Cyberspace

The concept of sovereignty has been a grand issue discussed by both social scientists and politicians from the past to the present. When the meaning of sovereignty is examined, according to Ayers (2016), the understanding of Sovereignty in the Western world is not only a political or juridical understanding but a combination of these two. According to the general approach in the world, the concept of sovereignty is explained in its simplest form as follows; Sovereignty is the supreme authority that will155 keep a government out of the intervention of other governments within the absolute boundaries of the country (Ayers, 2016).

This definition for the concept of sovereignty has its roots in the 1648 peace of Westphalia. According to some political scientists, the emergence of today's sovereign nation-states is a result of the Treaty of Westphalia. According to Creemers (2020), the international system created with the 1648 Peace of Westphalia was based on principles such as non-intervention in the internal affairs of other states and sovereign-equality. According to Ayers(2016), the Westphalian world

order was not fully functional due to the existence of empires and the irresistible understanding of colonialism until the end of World War II. The United States and the Soviet Union emerged as two superpowers after the World War II. While the colonial lands of Germany, Italy, and Japan, the defeated countries of the war, were completely liquidated or shared by other powers, the victors such as Britain, France, Belgium, and the Netherlands faced the growing liberation movements in their colonies at the same time (Çiftçi, 2018). Colonies countries which started the struggle for independence after the Second World War soon gained their independence and started their construction as a nation-state (Çiftçi, 2018). Most of the states, which gained independence from the colonial powers and launched to build a nation-state, adopted the Westphalian sovereignty understanding, which excluded any foreign intervention or actor within the borders of the country (Ayers, 2016).

Nowadays, with the development of information and communication technologies (ICT) and their incremental effect on human life, some new discussions have surfaced beyond the classical understanding of Sovereignty and the discussions made in this context. The most important of these discussions is sovereignty in cyberspace or in other words cyber sovereignty. Studies that analyzed the relationship between the Internet and the concepts of sovereignty have continued in the academic world since the 1990s (Zeng et al., 2017). According to Creemer (2020), in the early years of information and communication technologies (ICTs), the purpose of the development and use of these technologies was basically related to national security policies, such as espionage, surveillance, and projects such as Apollo, which would increase the country's prestige.

In the following years, with the increase in the use of ICTs by both the business sector and individuals, the absolute role and control of states on communication and information technologies began to evanesce (Creemers, 2020). In the 1990s, a group of American engineers and scientists developed the internet as we know it today, which was a turning point in terms of ICTs and their use because, in the United States, the internet was founded on ethical values such as freedom, transparency, and openness (Creemers, 2020). Although at first, the governments showed resistance to the internet approach based on libertarian principles, thanks to the moderate atmosphere that emerged after the end of the "Cold War", this libertarian understanding was also adopted by most of the governments (Creemers, 2020).

According to this techno-optimist view created by the internet based on libertarian foundations, cyberspace has become a new phenomenon in which the traditional understanding of government does not have an absolute role and control (Creemers, 2020). Issues such as cyberspace and the sovereignty of states in the cyber field have become crucial in international politics. According to Zeng (2017), cyberspace emerged as a radical sphere that has its own sovereignty beyond the powers and authorities of states. John Perry Barlow's "Declaration of the Independence of Cyberspace" defines states as "weary giants of flesh and steel". According to him, governments no longer have sovereignty in the digital domain (Morrison, 2009).

According to the Creemers (2020), technology businesses effusively embraced this narrative of openness which rejects strong government regulations and allows them to grow rapidly on a global scale. The initiative to attenuate the role of the state has become an explicit goal in many aspects of internet governance, for example, in the "ICAAN (Internet Corporation

for Assigned Names and Numbers)" and the "IETF(Internet Engineering Task Force)", the multi-stakeholder actors such as the technology and business communities, and non-governmental organizations became as important as governments (Creemers, 2020). Although the foundation of the İnternet was based on libertarian values, reducing the role and control of the governments in cyberspace and internet governance for the United States and most of the Western Democracies, it was not the case for some countries that supported Westphalian understanding of sovereignty in cyberspace like China, Russia, and Iran.

In sum, according to Zeng et al. (2017), cyber sovereignty and, more broadly, internet governance differ widely between states. What vital issue for one state may be seen as less important or insignificant for the other state. In this sense, the divergent apprehension of cyber sovereignty by states is the basis of behavior that creates political disputes between governments (Zeng et al., 2017). This is particularly significant in the relations between China and Western democracies, especially the United States (Zeng et al., 2017). The perceptions of the United States and China towards Cyber sovereignty and Internet governance are diametrically opposed. While in the United States advocates a self-sovereign, individual-centered, and market-driven cyber sovereignty, China advocates a border-based, state-centered, cyber sovereignty that emphasizes the responsibilities of individuals rather than the rights of individuals (Jiang, 2010). Additionally, China's approach towards cyber sovereignty aspires to maximize economic benefit while making sure there is no political risk for the one-party state (Jiang, 2010).

2. China's Notion of Cyber Sovereignty

China, compared to the western world particularly the USA, met with the internet a little bit later. The first use of the internet by the civil community in China began in 1982 when FTP (File Transfer Protocol) and IP (Internet Protocol) protocols became legible. (Negro, 2017). It is a symbolic and important development that in 1987 the "Internet Project of the Chinese Academic Network (CANET)" team sent an e-mail from China to the University of Karlsruhe in West Germany with the subject of "joining the world by crossing the great wall" (Negro, 2017). In 1990, "National Computing and Networking Facility (NCFC)" launched the project that aims to establish a direct link between China and the whole world and will form the basis of the "China Science and Technology Network (CSTNET)" in the future (Negro, 2017).

According to Negro (2017), the year 1990 is very important for the development of the internet in China because China started its first cooperation with the ARPANET internet center and registered the country's domain name ".cn." in the same year. Although China registered for the country's domain name in 1990, the official recognition of the internet in the country took place in April 1994. After the official recognition of the internet in China, it has developed and spread very rapidly (Negro, 2017).

According to Negro (2017), the first steps taken in the development of the internet in China were basically the steps aimed at economic development as the paramount animus. Early times of the development of the ICT industries, former president Jiang Zemin played a leading role (Meng & Li, 2002). According to Negro (2017), former president Jiang Zemin fully understood the relationship between the information society and economic development and therefore valued the investments in the field of ICT. Jiang Zemin emphasized the importance of ICT investments

in many of his speeches in the 2000s. The most notable of these speeches are, the opening speech of the "National People's Congress (NCP)" and the "Chinese People's Political Consultative Conference (CPPCC)" on 3 March: during the "16th World Computer Congress" on 21 August, and during a meeting of the "Central Military Commission (CMC)" on 11 December (Creemers, 2020).

Negro (2017) argued that during the leadership of Deng Xiaoping the development of information and telecommunication sectors were based on the adaptation of developed countries. Negro (2017) explained adaptation of technology from the developed countries with Gerschenkron's "advantage of backwardness" theory. According to the advantage of backwardness theory, backward countries such as China can achieve high-speed economic development by taking advantage of the development already made by developed countries (Jiang, 2010). As mentioned above during the Deng Xiaoping period, the adaptation of foreign technologies was the main policy however in the Jiang Zemin period, investments were made with the understanding of the "competitive edge of a late start" to make China a leader in the newest and sophisticated ICT industries (Creemers, 2020). As a result of all these policies and investments, China has become a country with a strong economy and a leading position in many of the ICT sectors.

The development and spread of the Internet have considerably transformed people's lives in the USA and the Western world. The most essential of these transformations is the increase in rights and freedoms. During the development of the Internet in China, the Chinese government sensed the Internet as a tool for economic goals, on the other hand, the Chinese government ensured to prevent the spreading of USA-centered understanding of the internet in the country and harm the existence and legitimacy of the communist party.

In this context, from Xi Jinping's leadership China started to promote its own understanding of Cyber Sovereignty, which is border-based, state-centered and, emphasizes the responsibilities of individuals rather than the rights of individuals (Jiang, 2010). China's idea of "Cyber sovereignty" is a high-profile resurgence of a concept first presented in a 2010 white paper called "Internet in China". The white paper interpreted that "China's Cyber sovereignty" means "in Chinese territory, the Internet is under Chinese sovereignty." The white paper said that all individuals and organizations operating in China are expected to comply with China's Internet laws and regulations (Tiezzi, 2014).

At the 2012 Budapest Conference on Cyber issues, China proposed five principles for international cooperation in cyberspace (Creemers, 2020). The first of these, sovereignty, defined as the right of each state to formulate its policies and laws in the light of its history, traditions, culture, and language (Creemers, 2020). The Wuzhen Declaration, published at the first "World Internet Conference" in 2014 argued that "We must respect the rights of every country in the development, operation and governance of the Internet, and avoid misuse of resources and technological powers to violate other countries Cyber sovereignty" (Zeng et al., 2017, p. 24).

At the second "World Internet Conference" held in 2015, Xin Jinping again highlighted the issues mentioned in the Wuzhen Declaration and stated that according to Cyber Sovereignty, surveillance or hacking activities against any sovereign society would not be tolerated. (Ayers,

2016, p. 58) At the Cyber Forum held in May 2016, Chinese ambassador Liu Xiaoming made a speech similar to Xi Jinping's speech in 2015, stressing the following issues:

1. All sovereign states have the right to make and choose their own way in internet development

2. All sovereign states have the right to develop their own model of regulation and enforcement in Internet-related matters

3. All sovereign states have an equal right to attend to international cyber governance

4. The approaches from the Cold War era and zero-sum games should be deserted

5. No state should intervene with the international relations of other sovereign states or engage in cyber actions that would endanger the national security of other states

6. Any arms race in cyberspace should be avoided (Ayers, 2016).

According to Creemers (2020), the most important document written about the sovereignty debate in cyberspace is found at the International Cyberspace Cooperation Strategy meeting held in 2017. In his book Creemers (2020), draws attention to three important normative principles of China's Cyber Sovereignty understanding.

Firstly, independent states can use their cyber sovereignty against other nations, which is a response to the understanding of online openness, which is a general acceptance in the world. This principle explains that the state has the right to regulate and control all activities within its borders, including the opposing ideas such as free expression and access to information in cyberspace (Creemers, 2020).

The second principle argues that the state has absolute and full sovereignty over all cyberspaces. This principle makes it clear that any multi-stakeholder actor such as civil society organizations or non-state organizations should not have any control over internet governance (Creemers, 2016). According to this principle even though technical and trade institutions play an important role in internet governance the final decision should be made by nation-states through inter-governmental organizations (Creemers, 2020).

The third principle of what Creemers (2020), defined as normative dimensions of China's Cyber sovereignty is that all the sovereign states have equal participation in Internet governance, no states should have more rights than others or be in the quest for hegemony.

Apart from the normative principles of China's Cyber sovereignty Creemers (2020), also mentioned the domestic measures of China's Cyber sovereignty which he defined in his book as "The Capability Dimensions" of China's Cyber Sovereignty. The essential purpose of these domestic measures is to guarantee sovereignty at home for Chinese society even though there is no international adoption. According to Creemers (2020,), it is possible to gather these measures around three fundamental concepts: territorialization, indigenization and, investment (p. 122-131)

Territorialization refers to the territorial borders of cyberspace. From the techno-optimist view there is no border presence in cyberspace however the Chinese government has taken the opposite discourse to this view (Creemers, 2020). According to the CAC director, Lu Wei cyberspace is an appendage of the physical space for this reason it should not be excluded from the legal arrangement. The Great Firewall of China, hardware that basically controls the flows of the information, can be taken as a sample of implementation of this measure (Creemers, 2020).

The second measure, indigenization, aims to enhance the market share of Chinese companies in the manufacture of the technologies used in China (Creemers, 2020). According to the report published by party journal in 2014, 82 percent of the servers, 73.9 percent of storage equipment, 91.7 percent of databases and, 95.6 percent of operating systems in China are driven by foreign enterprises (Creemers, 2020). The article points out the vulnerability of China towards foreign-sourced enterprises in the technologies used in cyberspace. For instance, in 2014 Microsoft announced that it will withdraw its support from the Windows XP system while the Windows XP was still used by most Chinese users (Creemers, 2020). To prevent this vulnerability China's government developed indigenization as a key component and increases the investment and support for China's own ICT companies such as Huawei, Vivi, Xiaomi and, Oppo. Owning to this massive support and a large amount of investment, some of these companies become leader status of the ICT sectors such as Huawei in 5G technologies (Creemers, 2020).

With the favor of these three measures, China's notion of Cyber sovereignty was adopted and implemented in China successfully. The adaptation of the Cyber sovereignty just by China itself, however, not enough for the ambitious Chinese government. Since the United States has already taken the hegemon position of cyberspace for many aspects and in many countries the only way to change this status quo, from the Chinese perspective, could be the international adaptation of Chinese notion of Cyber Sovereignty. Thus, to increase adaptation of its understanding of Cyber Sovereignty China targeted developing and underdeveloped countries as potential recipients.

3. Legislative and Technical Actions to Implement Cyber Sovereignty in China

According to Tai (2005), the world has witnessed a global revolution in the last two decades thanks to Information and Communication Technologies. China, like many other states, realized the socio-economic transformation created by technological developments and accelerated its investments in this field (Tai, 2005). According to Thomala (2021), China hosts the world's largest digital community with 989 million internet users. The Chinese government is aware of the benefits of ICTs that develop with the internet for the country's economy, as well as the risks that this technological transformation may create.

The existence and legitimacy of the party, undoubtedly, comes first in Communist China. Both economic and any other policy often serve a single essential purpose; preserving the existence and legitimacy of the party because, for the Chinese government, the existence of the party means the existence of the whole state. Tai (2005), underlines that, in the policies of development of internet and ICTs, as in all other policies, China's primary goal was to make sure that the party's authority would not be damaged while gaining economic advantages that comes with the internet.

According to Tai (2005), China actually revealed its intention to control the Internet and the cyber space from the very beginning with the regulation titled "Regulation for the Protection of Computer Information System" in 1994. Since its first regulation to control the internet in 1994, China has managed to keep cyberspace systematically under control in many different levels. (p. 140-143) Discussions about the need for Internet monitoring and control in China began in the mid-1990s (Negro, 2017).

The first document on the regulation of cyberspace in China, named "Regulation for the Protection of Computer Information System and Safety" was published September 18, 1994 (Negro, 2017). In this revision published by the "State Council, The Ministry of Public Security" was defined as the main body of the administration, and it was emphasized that the primary task of this body was to supreme to the infrastructure and investigate online criminal activities (Negro, 2017). Tai (2005), states that the essential point of the regulation made in 1994 was to control physical entity of the information system in the country however, the regulation did not give much attention to content control. (p. 141)

Before long, the Chinese Government realized that content control was also very important, and the State Council published the first official regulation for content control with the title "Implementation Measures for Enforcing the Temporary Decree on the Management of Computer Information Network International Connectivity in the People's Republic of China" (Tsui, 2003). This regulation, which was organized in February 1996 but started to be implemented in 1997, stated that the use of the Internet to produce harmful and obscene content that could harm the People's Republic of China is forbidden (Negro, 2017). According to Tai (2005), the problem with this regulation wasn't that it was controlling the content, because all nation-states may want to ban content that would harm the country, but the problem with this regulation was that the government did not fully explain what types of content would be deemed harmful. Therefore, in this way, the government would be able to evaluate the information in cyberspace as harmful and harmless in its own interest.

Negro (2017) highlighted that another important regulation made for the control of the internet was the "State Secrets Protection Regulations for Computer Information Systems on the Internet" published by "National Security Bureau" in January 2000. (p. 64) According to this regulation, sharing state secrets or discussing state secrets online was prohibited. In addition, it was underlined that all these IPSs and ICPs organizations were forced to obtain security certification and they considered responsible for the security of the state (Tai, 2005). Tsui (2003), emphasizes that, as in other regulations, the concepts were not fully explained in this regulation. Sharing state secrets online was not welcomed by any state nation, but the important issue here was what kinds of information would be considered state secrets, but the Chinese government did not clearly explain this in the regulation. According to Tsui (2003), since the concept of state secret could be expanded in many different ways, not fully disclosing it would increase the perception of "stay on the safe side" among the public and a natural control mechanism would have been formed for the Chinese Government. (p. 39)

Another important development in the regulation of cyber space in China is the establishment of the country's first Cyber Police Force in Anhui province in August 2000 (Tai, 2005). The main task of the Cyber Police Force defined as administrating and sustaining the order on computer networks (Negro, 2017). The application, which first started only in Anhui province in 2000, was initiated by other regions in a short time. By the end of 2000, it was reported that there was 300,000 active cyber police force in China and about 12 million people were monitored (Negro, 2017).

In addition to these regulations, in order to strengthen internet control, the Ministry of Information has published a statement demanding all website owners operating in China to register with Chinese authorities by June 2005. At the end of the time given by the Chinese government, about 1000 websites were closed for not meeting this requirement (Tai, 2005). According to Tai (2005), companies that do not want to comply with the Chinese government's regulations were quickly punished. The best example of this would be Google, which was frequently used by Chinese users but suddenly banned to access in August 2002 by the Chinese government because of Google refusal to implement the filter policy of the Chinese Government. Google later backs out and accepts the terms of the Chinese government but was banned again for another dispute in 2010.

Eventually, Tai (2005) states that the simplest way to control unsolicited content is to block it altogether. This is the motivation behind the Chinese "The Golden Shield Project" which is World's most sophisticated blocking and filtering system (Negro, 2017). In another word, The Golden Shield project is the technological implementation of legislative regulations on İnternet control. The Great Firewall is the name given to the project by the Western World because of Its structure. The official name of it is "The Golden Shield Project" which first occurred in 1996 but started to be fully implemented in 2006 (Chandel et al., 2020). Tsui (2003) states that the essential reason for the launch of "The Golden Shield Project" is to increase the adaptation of information and communication technologies to catalyze content control in cyberspace and to strengthen the combat against crime in the cyber space.

According to Chandel et al. (2020), the Golden Shield Project, which has occurred for so-called reasonable reasons, has turned into a highly sheltered, heavily monitored, fully controlled system that deserves to qualify as "The Great Firewall". The name "Golden Shield" given to the project by the "Ministry of Public Security" and the main purpose of the project explained to combat and protect China's İnternet from harmful and illegal content mostly from outside of the country (Negro, 2017). From the day the Golden Project became fully active, dozens of web pages, IPs, and URLs were blocked including the most popular social media applications such as Twitter, Facebook, Instagram. (Chandel et al., 2020).

According to Chandel et al. (2020), the development of "The Golden Shield Project" can explain in four phases. Chandel et al. (2020) state that, the first phase of The Golden Shield Project started with the blocking of some specific domain names and IP addresses within the country. "The Golden Shield System" used to identify users who violated this rule. For the effective implementation of this practice, Chinese officials asked all internet cafes in the country to install spying software approved by local authorities on their computers. In this way, the state gained the ability to monitor all the transactions of computers in internet cafes (Chandel et al., 2020). In addition, Chinese authorities required all internet cafe users to register with an ID card before using computers so that people who violate the rule can be identified and punished immediately.

According to Chandel et al. (2020), the second phase of The Golden Shield project started with the application of key-word filtering. With the implementation of this application, internet users who make a search on the content designated as "sensitive content" are directly disconnected from the content (Chandel et al., 2020). The third phase of The Golden Shiel Project is the blocking of the most widely used VPN providers such as Free VPN and Tianxins VPN by

the system upon the realization that some internet users violate the bans using VPN . The fourth phase of Great Firewall development in China is to introduce legal regulations that will penalize VPN providers in order to prevent violations of the bans on Internet Use through VPNs (Chandel et al., 2020).

As a result, with all these developments and increased controls, The Golden Shield Project turned into The Great Firewall, the world's most advanced content control system. The Firewall plays an essential important role for China to legitimate what they call İnternet Sovereignty. While China sees The Great Firewall as a tool to protect their Cyber sovereignty, for the USA and the Western World, this system and the Chinese model of Cyber Sovereignty are the efforts of the Chinese government to legitimize its repressive policies.

4. The Internet in China as a Tool of Social Management

From the early years of development of the Internet in China, Chinese leaders were aware of the damage that the Internet's impact on society could cause to the Communist Party, and for this reason, they aimed to make the Internet and all technologies developed with the Internet controllable and accountable by turning it into a social management tool. Zeng et al. (2017) states that, in many of the official documents published by the Chinese government especially after 2010, special emphasis is placed on issues such as "stability", "public security", "legitimacy of the CCP".

According to Zeng et al. (2017), the reason of Chinese government's behavior can be seen as response to the global revolution that has emerged with the development of technology. The Communist Party of China sees the existence and legitimacy of the party as the source of stability in the country and they believe that the party's existence can be guaranteed by strong social management.

According to Creemers (2020), the internet is one of the most important tools for social management because the government can be more powerful and resourceful online, while also being less direct and invasive. China's use of the internet and other advanced technologies to keep society under control is realized through both government official institutions and private technology companies. "The State of Information Office", which was established in 2011 is being at the head of China's advanced internet censorship mechanism. Besides this official institution, leading state-owned telecommunications companies China Telecom, China Unicom, and China Mobil are also important constituents of the internet censorship system.

One of the most important milestones in the Internet's becoming a surveillance tool in China is the "Cyber Security Law" issued in 2017. With this law, all technology companies operating in China have become responsible for their customers' cyber activities. According to this law, all technology companies had to monitor their customers' activities and report of the authorities if any illegal activity is carried out (Internet Censorship in China Explained - Daxue Consulting - Market Research China, 2020). As a result of both the legal regulations and the cooperation of the Chinese government with the main telecommunications and internet providers, China has succeeded in transforming the internet, which was initially supposed to change the system by increasing freedoms, into a tool of social management. According to the Market Research's report, 6,000 websites in 2018 and 733 websites in January 2019 alone were shut

down by the Cyberspace Administration of China for violating regulations (Internet Censorship in China Explained - Daxue Consulting - Market Research China, 2020). In addition, 9,382 mobile apps and more than 7 million pieces of information were removed from the online environment for the same reason.

In addition to censorship activities to increase social management, the Chinese government also uses "face recognition technologies" as a control tool. W. H. Gravett (2020) argues that China is the country where facial recognition technologies are developing the fastest in the world because the Chinese government has understood the great potential of these technologies in social management. Facial recognition technology is a very advanced technology that helps to identify the facial features of a person in less than a minute, to distinguish that person from thousands of other people, and to provide a lot of information about the person by making potential matches (W. H. Gravett, 2020). Thus, facial recognition technologies are a unique opportunity for the Chinese government, which is trying to make the internet and the technologies that develop with the internet a tool to keep society under control.

On this basis, the Ministry of Public Security of China started a project in 2015 to develop the world's most advanced facial recognition system. According to the ministry's statement, when the project is completed, the system will have the capacity to analyze the data of 1,393 billion Chinese citizens within just three seconds (Dong, 2012). In addition to this project, it is known that the Chinese government already uses facial recognition technologies to control the people especially in areas where minorities live. According to the Chinese government's argument, authorities are using facial recognition technologies for the benefit of society to combat "terrorism, separatism and extremism", which the government has identified as the three evils (W. Gravett, 2020, p.18). However, according to many Western human rights institutions, since the Chinese government does not clearly define the scope and limits of the concepts, the use of facial recognition technologies becomes a means of control, espionage, and assimilation, far beyond combating "terrorism, separatism and extremism" (W. H. Gravett, 2020).

As a result, the Chinese government used the Internet for socio-economic development with the discourse of "cyber sovereignty", while it reduced the political risks and made the Internet a tool of social management. Although many Western states, especially the USA, are against the high rate of state censorship, "China's notion of cyber sovereignty" argues that all states have the right to choose their own path of cyber regulation and development of public policies for the internet.

Conclusion

In the 1990s, a group of American engineers and scientists developed the internet based on ethical values such as freedom, transparency, and openness (Creemers, 2020). Although at first, the governments showed resistance to the internet approach based on libertarian principles, thanks to the moderate atmosphere that emerged after the end of the "Cold War", this libertarian understanding was also adopted by most of the governments (Creemers, 2020). According to this techno-optimist understanding, cyberspace has become a new phenomenon in where the government does not have an absolute role and control. However, this new understanding of the Internet which did not accept the absolute control and sovereignty of the governments in

cyberspace was not suitable for all the states. Undoubtedly China was one of these states. In the early years of adaptation of the internet in China, the Chinese government discerned the internet and related technologies as only a tool for high economic development. For this reason, the Chinese government did not want to miss the opportunities that the internet would create. However, at the same time, the Chinese government was aware of the possible harm that USA-centered understanding of the internet based on a libertarian foundation, would create for the legitimacy of the Communist party. Thus, the Chinese government needed to develop its understanding of cyber sovereignty, with its characteristic which is opposite to the techno-optimistic view to control the spread of the internet in China. In this regard, the concept of Chinese cyber sovereignty first appeared in the White Paper published in 2010, although its applications have been seen since the early years of the Internet's adaptation in China. The White Paper defines the Chinese notion of cyber sovereignty as: in Chinese territory, the Internet is under Chinese sovereignty, all individuals and organizations operating in China are expected to comply with China's internet laws and regulations (Tiezzi, 2014).

Thanks to the practices of this cyber sovereignty, China prevented the spread of the internet based on American values which expected to lead the collapse of the Chinese Communist Party. Since the internet, for the Chinese Government, is seen as tool for economic development and used for this goal, the Chinese government achieved increased economic welfare and stability of the people. Thus, this leaded the Chinese government to increase the party's legitimacy thanks to the internet and concept of the cyber sovereignty.

Consequently, although the Chinese government still has many legitimacy lacks, mainly in corruption, rule of law, public safety, and social inequality, the party is still viewed legitimately by most Chinese netizens. (Jiang, 2010) From the government's viewpoint, although the Internet poses some significant challenges to the government, it is possible to overcome such challenges and secure its survival by producing economic growth, social stability, and national identity. In this regard, the Chinese government aims to use the Internet not only to increase its authority in society but also to enhance its legitimacy.

Çıkar Çatışması: Yazar(lar) çıkar çatışması olmadığını beyan eder.
Disclosure Statement: No potential conflict of interest was reported by the author(s).

References

Ayers, C. E. (2016). '*Rethinking Sovereignty in the Context of Cyberspace*' (2nd ed.). United States Army War College. https://www.hsdl.org/?view&did=802916.

Creemers, R. (2020). 'China`s Conception of Cyber Sovereignty: Rhetoric and Realization.' in Broeders, D. & Berg, B. (Eds), *Governing Cyberspace: Behavior, Power and Diplomacy.* London, England: Rowman & Littlefield. 10.1007/978-3-319-60405-3. (pp. 107-145).

Chandel, S., Zang J., Yu Y., Sun J., and Zhang Zhipeng. (2020). 'The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall,' 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, (pp. 111-119). 10.1109/CyberC.2019.00027

Negro, G. (2017). 'The internet in China: From infrastructure to a Nascent Civil Society.' Gham, Switzerland: Springer International Publishing AG. DOI 10.1007/978-3-319-60405-3

Tai, Z. (2005). The Internet in China: Cyberspace and Civil Society. New York, USA: Routledge Taylor & Francies Group.

Çiftçi, K. (2018). 'Millet - System Versus Westphalia - System and International Politics in The Post -Cold-War Period.' Karadeniz Sosyal Bilimler Dergisi, 8325, 0– 2. (pp. 1-21). 41531/501301

Gravett, W. (2020). 'Digital neo-colonialism: The Chinese model of internet sovereignty in Africa.'

African Human Rights Law Journal, 20(1) (pp. 125–146). https://doi.org/10.17159/1996-2096/2020/v20n1a5

Gravett W. H. (2020). 'Digital Coloniser? China and Artificial Intelligence in Africa', Survival, 62(6): (pp. 153-178), DOI: 10.1080/00396338.2020.1851098

Goldsmith, J. L. (1998). The Internet and the Abiding Significance of Territorial Sovereignty. *Indiana Journal of Global Legal Studies*, *5*(2), 475–491. http://www.jstor.org/stable/25691116

Jiang, M. (2010). 'Authoritarian Informationalism: China's Approach to Internet Sovereignty.' SAIS Review of International Affairs, 30(2): (pp. 71–89). https://doi.org/10.1353/sais.2010.0006

Morrison, A. H. (2009). 'An impossible future: John Perry Barlow's "Declaration of the Independence of Cyberspace.' New Media and Society,11(1–2):(pp. 53–71). https://doi.org/10.1177/1461444808100161

Zeng, J., Tim S., and Yaru C. (2017). 'China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty.' Politics and Policy, 45(3): (pp. 432–464). https://doi.org/10.1111/polp.12202

Internet Censorship in China Explained. (2020, May 11. Daxue Consulting - Market Research China. Retrieved from https://daxueconsulting.com/internet-censorship-in-china/

Tiezzi, S. (2014, June 24). China's 'Sovereign Internet' .The Diplomat. Retrieved from https://thediplomat.com/2014/06/chinas-sovereign-internet/

Tai, Z. (2005). The Internet in China: Cyberspace and Civil Society. New York, USA: Routledge Taylor & Francis Group.

Thomala, L. L. (2021, February 11). Internet usage in China - statistics & facts | Statista. Statista. Retrieved from https://www.statista.com/topics/1179/internet-usage-in- china/

Tsui, L. (2003). 'The panopticon as the antithesis of a space of freedom: Control and Regulation of the Internet in China.' China Information, 17(2): (pp. 65–82). https://doi.org/10.1177/0920203X0301700203

Dong, F.(2012). 'Controlling the internet in China: The Real Story.' The International Journal of Research into New Media Technologies, 21(4): (pp. 1-23). 10.1177/1354856512439500