SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 01 No. 02 (2024), pp. 164-177
Research Article
doi: https://doi.org/10.70710/sitj.v1i2.23

China's Cyber Security Governance as Part of Foreign and Security Policy

Mira Murniasari[1,a,*]

[1]Sekolah Tinggi Intelijen Negara (STIN), Bogor
[a]miramengniya@gmail.com
*Corresponding author

Article Info
Received: 28-Nov-2024
Revised: 28-Nov-2024
Accepted: 01-Dec-2024

Keywords
China; Cyber; Security

Abstract
Cyberspace has become a new method of interaction for humans in the digital industrial era. One of the countries that play an important role in global cyberspace is China, which has the largest number of internet users, reaching 989 million. This has prompted the Chinese Government to formulate a complex cybersecurity governance strategy to maintain national stability and security. Therefore, this study aims to explore China's approach to cybersecurity at domestic and foreign levels. The domestic level explores the governance of the country by examining strategic documents, policies, and legal and institutional frameworks. In contrast, the foreign level discusses cybersecurity as part of foreign and security policy. The primary focus of this study is the series of Chinese diplomatic initiatives aimed at shaping governance norms across various international forums.

1. Introduction

The world's growing interconnectedness through the internet presents new challenges to China's national security. In December 2010, China had a total of 457 million internet users, with 98.3% of citizens being connected to mobile broadband connections. In the same year, more than 160 million citizens engaged in shopping through online applications. These data show that the country is closely associated with the Internet, presenting valuable infrastructure in terms of bureaucracy, economy, and communication. However, it also presents a high risk of cybersecurity problems (Fei, 2011).

Since the beginning of Xi Jinping's tenure in 2012, the government has paid special attention to cyberspace. Institutionally, China established the Central Cybersecurity Commission and Cyberspace Administration in 2014. The 2 institutions are tasked with managing cyber policy coordination between Chinese state institutions while also playing a significant role in the formation of cyberspace laws (Creemers, 2019).

In the context of foreign policy, the cyber approach is seen as an effort to support the internationalization of China's economic and political interests. Initially, the country implemented a cybersecurity concept that refers to the New Security Concept. This new concept means that China views security relations with a long-term approach and respects the national interests of other countries. Consequently, the country prioritizes mutual trust, mutual benefit, common interests, and inter-state consultation methodology in the context of cybersecurity. This method emphasizes multilateral efforts to achieve shared cybersecurity goals (Fei, 2011).

After Xi Jinping's rise as China's leader, cybersecurity in the context of foreign policy aims to support 2 national interests, namely commercial or economic and political. The international commercial interest

can be seen in the presence of the Belt and Road Initiative (BRI). Although BRI focuses on infrastructure and logistics cooperation, information technology also plays an important role in this grand plan. In the framework of the Digital Silk Road (DSR), cyberspace has become an important economic instrument for international commercial interests in BRI. The existence of DSR presents various vulnerabilities that are anticipated through the One Belt One Road Digital Economy International Cooperation Proposal offered by China at the 2017 Wuzhen World Internet Conference. The proposed cooperation in the BRI framework also carries the country's political interests in the international arena because the proposal aims to invite collaboration between countries to achieve harmonization of digital economies (Creemers, 2019).

According to previous studies, efforts in China's foreign policy have an impact on its relationship with the United States (US), which considers cybersecurity as a zero-sum framework. In addition, the concept of data and internet sovereignty spread by China has been a subject of debate, not only between the 2 countries but also with the European Union (Creemers, 2019).

2. China and Cybersecurity

A recent trending topic is China's approach to cybersecurity governance, which emphasizes the concept of "internet sovereignty." The White Paper "The State of China's Internet," published in 2010, stated that the Internet operating in China was under the sovereignty and jurisdiction of the Chinese state. The implication was that the state was considered to have absolute and exclusive rights to control internet use at the domestic level. Several academics believed that this condition was created to address the insecurity of the Chinese Communist Party (CCP) regime following the widespread use of the Internet. From the CCP's perspective, the Internet could increase threats to the regime's security, both from domestic activities and external influences. This perception was also supported by the widespread discussion of several Chinese academics who categorized international phenomena such as the Arab Spring and the collapse of the Soviet Union as real consequences of minimal government control over the circulation of information in their country (Ye & Zhao, 2014; Ran, 2017).

As a control mechanism, policies such as domestic internet censorship were intended to suppress the spread of public views that were contrary to the government, as well as foreign ideas considered to have the potential to delegitimize CCP and destabilize the country (Zeng et al., 2017). For an authoritarian country such as China, these factors must be implemented to maintain regime stability. The concept of internet sovereignty was introduced to justify this authoritarian policy. Although it is not free of criticism from the grassroots, the Chinese government could be said to have succeeded in gaining public compliance and strengthening its political position in the country's cyber regulation. A survey conducted by the Pew Study Institute in 2007 on Chinese internet usage found high public trust in government regulation of the internet. A total of 75% of respondents said information on government websites was more trusted than other online sources of information (Fallows, 2008).

This condition was closely related to how the Chinese government fostered public trust in the government, which had succeeded in making various efforts to maintain the stability of economic performance, nationalism, ideology, culture, and government as sources of regime legitimacy that shaped public compliance (Jiang, 2010). By examining this pattern, China still adhered to the "authoritarian informationalism" approach, namely a model of information development and regulation that combined elements of capitalism, authoritarianism, and Confucianism (Jiang, 2010). These 3 elements were considered capable of producing economic growth, social stability, and national identity, which were the aspirations of Chinese people. This was an opportunity for the Chinese government to utilize the internet as a tool to increase its legitimacy.

Efforts to increase the legitimacy of this regime were not only carried out at the domestic level. McKune and Ahmed's (2018) paper examined how China began to promote the norm of cyber sovereignty to the international world as an alternative to contemporary global cybersecurity governance, which was considered to be dominated by the US and Western countries. In this case, China sought to establish alliances with developing countries to gain international support for the concept of Internet sovereignty and the accompanying digital authoritarian practices (McKune & Ahmed, 2018). Efforts to disseminate this norm began by utilizing the Shanghai Cooperation Organization (SCO) as a regional organization capable of facilitating the dissemination of norms at the international level. Together with SCO member countries, China attempted to introduce the International Code of Conduct for Information Security at the UN General Assembly in 2011 and 2015 (McKune, 2015).

The presence of SCO members as supporters then encouraged China to propose the International Cyber Cooperation Strategy in 2017. This strategy was the first and only official international strategy related to cyber issues released by the Chinese government to date. In this strategy, this country encouraged the development of a multilateral, democratic, and transparent global cyber governance system (Ministry of Foreign Affairs and Cyberspace Administration of China, 2017). The 3 principles were used in global cyber governance; however, when they tended to be used by Western countries for domestic regulatory purposes, China emphasized the use at the international level (Cuihong, 2018). While the West interpreted the multi-stakeholder principle as a recognition of the participation of non-state actors, China interpreted it as a principle to emphasize the equal participation of all countries in global cyber governance. While democracy was intended to maintain the free flow of information within a country, it interpreted democracy as a principle to avoid competition that could be caused by imbalances in internet capacity between countries. In addition, while the principle of transparency refers to the openness of countries regarding internet management, China saw that transparency must be applied to the structure of global cyber governance (Cuihong, 2018).

Another form of implementation of China's alignment strategy was the establishment of the "World Internet Conference" held in Wuzhen, China, in 2014. This brought together state leaders, leaders of technology companies—including Facebook, Amazon, Google, Apple, Alibaba, and Tencent—think tanks, and other important figures in the internet community to discuss the direction of global internet system regulation. This forum also served as a place for China to promote the progress of its technology industry and re-emphasize the principles of internet sovereignty (McKune & Ahmed, 2018).

Despite its active role, China still faces several challenges in promoting internet sovereignty in global cybersecurity governance. Zeng et al. (2017) stated that the formulation of China's concept of Internet sovereignty still tended to be fragmented, diverse, and underdeveloped. This was mainly due to China's inconsistent policy formulation pattern, where political ideas were often not clearly defined when first proposed by its leaders. At the domestic level, there was still substantial debate over the definition and application of the concept of internet sovereignty. China's policies often contradicted its internet sovereignty commitments (Zeng et al., 2017); for example, it emphasized the principle of non-interference in the internal affairs of the state. However, China itself often used extraterritorial digital intrusions to achieve its regime interests. This misalignment then had the potential to hamper China's capacity to compete with contemporary global cyber norms as it aspired.

3. China’s Cybersecurity Policy Changes Direction

Since first connecting to the global internet network in 1994, there has been a shift in China’s cyber governance priorities and approaches. Initially, policy priorities were directed at infrastructure development, information system security, and industrial development (Miao & Lei, 2016, p. 337). Along with domestic social developments, the increasing number of internet users, and the need to narrow the economic gap between societies and China’s growing political influence internationally, the Chinese government began to recognize the importance of monitoring content in cyberspace.

The year 2014 was a turning point for China’s cybersecurity policy. In February, President Xi Jinping, speaking at the Central Leading Group (CLG) for Informatisation, expressed the view that internet security and informatization had become key strategic issues concerning national security and development (Panda, 2014). China, according to President Xi Jinping, must do everything it can to become a “cyber power” (Xi Wants China to Be “Cyber Power,” 2014). President Xi Jinping’s speech could be seen as a political commitment that underlined the structural reform of China’s cybersecurity governance and its approach to global cyber governance, as explained in the following sections of this study.

China’s cyberspace governance could be explained from several perspectives. First, as Jiang (2010) writes, China’s internet development and cyberspace regulation policies combined elements of capitalism, authoritarianism, and Confucianism, or what was called “authoritarian informationalism.” According to this model, the internet inherently posed fundamental challenges to the regime's legitimacy. However, these challenges were mitigated by promoting economic growth, social stability, and national identity. Ultimately, the Chinese government hoped to use the internet not only to strengthen its control over society but also to strengthen its legitimacy (Jiang, 2010). Second, and related to the first, China’s approach viewed cybersecurity or information security as part of national security. This meant that it was seen as a process or effort to minimize risks or threats to a particular reference object, be it a state or society arising from

activities in cyberspace (Austin, 2017). In 2013, President Xi Jinping said that the Internet was directly related to national ideological security and regime security (Miao & Lei, 2016). In other words, the speech at the CLG in 2014 could be seen as a directive from the highest political leadership that allowed for the mobilization of all resources needed to achieve China's national interests in cyberspace.

The structural changes that had occurred in China's cybersecurity governance following President Xi Jinping's directive to make the country a cyber superpower by all means were essentially driven by a sense of insecurity. There were at least 3 contexts of insecurity that explained the change in the direction of China's cybersecurity policy. First, the very significant increase in the number of internet users had the potential to change the shape of state-society relations and presented challenges to the legitimacy of the regime (Zeng et al., 2017, p. 437). As mentioned in the previous section, China is currently the country with the largest number of Internet users in the world, with around one billion of its population connected to the Internet.

Regime insecurity has long been a concern for political leaders in China (Zeng, 2015). From the perspective of the CCP regime, the development of information and communication technologies heightened this concern, as Chinese society now had more opportunities to create, discover, and disseminate information that contradicted the narratives constructed by the government (Zeng et al., 2017 p. 438). The transnational nature of the internet had enabled the "invasion" of Western liberal ideas such as democracy, which were seen as endangering the legitimacy of the one-party system and the centralization of political power in China (Zeng et al., 2017, p. 438).

Secondly, there was an emergence of awareness that China was still lagging behind its competitors, specifically the US, in terms of cyber power (Austin, 2016, p. 5). This was mainly triggered by the increasing cyber espionage activities carried out by the US, as well as the development of US military cyber capabilities, which were considered a threat by the Chinese government. In 2013, Edward Snowden, a former consultant at the US National Security Agency, shocked the public by stating that the US government had hacked Chinese mobile phone companies to collect various user data, including phone calls and browsing data (Rapoza, 2013). Furthermore, according to Snowden, the US government also spied on Tsinghua University, where the China Education and Study Network (CERNET) was located, one of China's 6 main backbone networks. Access to CERNET could provide a hacker with data on millions of internet users in China (Rapoza, 2013).

Thirdly, public activism on cyber threats and cybersecurity at that time was not accompanied by a strong institutional infrastructure. In 2013, President Xi Jinping highlighted several problems in China's Internet governance, including overlapping authorities and functions of several institutions and inefficient management. The issue of institutional structure could be discussed in more depth in the next section.

The National Cybersecurity Strategy document outlined 4 principles underlying China's cybersecurity strategy (Full Text of "National Cybersecurity Strategy," 2016). First, respect and protection of sovereignty in cyberspace. Every country, according to China, has the right to select the direction of its cyber development, formulate cyber regulations based on its conditions, and participate equally in international cyber governance. China rejected any attempt to realize cyber hegemony, the application of double standards, the use of the internet to interfere in internal affairs, and support for cyber activities that endangered the national security of other countries.

Second, the use of cyber for peaceful purposes in which China rejected the use of national security as a pretext to control other countries' networks and information systems, the collection and theft of other countries' data, and attempts to achieve absolute cybersecurity at the expense of other countries' security. Third, cyberspace management is based on law; although having freedom and rights in cyberspace, every person and organization must obey applicable laws, respect the rights of others, and be responsible for their words and actions in cyberspace. Fourth, coordination between network security and development. Chinese government viewed security as a prerequisite for development and, vice versa, development as a foundation for development. In the cyber realm, the development of informatization was seen as an effort to realize network security. In the National Cyber Security Strategy, the Chinese government also outlined 9 "strategic tasks" in cybersecurity governance.

Table 1. The Nine NCSS "Strategic Tasks," Source: (Austin, 2018)

NCSS's Nine "Strategic Tasks"	Description
Maintaining cyberspace sovereignty	Political security and regime
Upholding national security	
Protecting critical information infrastructure	Resilience of digital economy and public services
Strengthening online culture	Countering rumors and fake news; strengthening digital culture; regulating communication ecosystem
Eradicating acts of terrorism and cybercrime	Protecting government agencies, corporations, and individuals from cyber attacks and information theft
Enhancing cyber governance	Law enforcement, mobilization of all stakeholders
Strengthening cybersecurity foundations	Cybersecurity industry policy and education
Strengthening cyberspace defense capabilities	Preventing cyber-based invasions in war and peace
Strengthening international cooperation	Diplomacy and norm promotion

As in other sectors, China's cyber governance was state-centered. In this model, the central government held the greatest power in regulating cyberspace, from infrastructure to content (Miao et al., 2021, p. 2005). Commercial, non-governmental, and civil society entities played complementary roles (Miao et al., 2021, p. 2005). However, in the government bureaucracy, competition between institutions had resulted in what was called fragmented authoritarianism, where the government did not act as a single entity but rather consisted of a complex system of power and control, and bureaucratic institutions competed for influence and autonomy (Miao et al., 2021, p. 2005).

In the 1990s, when China was still trying to understand the potential of the Internet for development, internet governance focused on industrial and technological development. As a result, the Ministry of Information Industry became the most powerful regulatory agency at that time (Miao et al., 2021, p. 2006). Then, in the 2000s, as the internet played an increasingly important role in communication and public opinion formation, agencies responsible for "ideological security," such as the Ministry of Culture and media watchdogs, began to take on greater roles (Miao et al., 2021, p. 2006). In 2010, the State Council Information Office established the Internet News Regulatory Bureau. As mentioned in the previous section, the duties and functions of this agency demonstrated China's cybersecurity policy approach during that period, which focused on controlling and monitoring content.

Entering the 2010s, the Chinese government began to realize the need to organize a more streamlined and effective, but also comprehensive, cyber governance system. The duties and functions of the Internet News Regulatory Bureau were then replaced by the State Internet Information Office in 2011 (Miao & Lei, 2016, p. 337). This change showed the Chinese government's intention to develop a comprehensive cyber governance system beyond just content management. Finally, in 2014, cybersecurity was officially elevated to part of national security, which required the formulation of policies and strategies at the highest level of government. In implementing structural reform of cybersecurity governance after 2014, instead of building from scratch, the Chinese government chose to make changes and developments to the existing structure. With this approach, existing units were renamed, organized, and assigned tasks and functions, and their command relationships were changed. Essentially, these structural changes were a reflection of China's perception of threats, national interests, and changes in the direction of cybersecurity policy.

Since cybersecurity was considered a strategic issue and part of the national security discourse, the national security apparatus—military, homeland security, law and order, and intelligence—held a key position in China's cybersecurity governance (Cheung, 2018, p. 2). The following section describes some key agencies in China that had authority in the field of cybersecurity, along with the reasons for their establishment and their main tasks and functions.

In February 2014, President Xi Jinping initiated a more significant structural reform of China's cybersecurity governance. In addition, to realize China's aspiration to become a cyber superpower, President Xi Jinping established the Cyberspace Administration of China (CAC). Structurally, the CAC served 2 functions simultaneously in the CCP hierarchy and state administration. First, the CAC was subordinate to the Central Cyberspace Affairs Commission (CCAC), an agency established under the Central Committee of the Chinese Communist Party (CCCPC) that was tasked with formulating and implementing policies to manage internet-related issues. The CCAC was chaired directly by Xi Jinping, who was the General Secretary of the CCCPC. In this capacity, the CAC served to provide support for CCP policies. Second, this also served as a semi-military institution under China's State Council. In line with this dual function, at the time of its establishment, the 2 deputy director positions of the CAC were filled by Le Keqiang, as Premier of the State Council, and Liu Yunshan, as Head of CCP Central Propaganda Department. Both were also members of the CCP Politburo Standing Committee, the body that contained the CCP's top leadership.

The establishment of the CAC was one of the most significant structural changes following the reorientation of China's cybersecurity policy in 2014 (Austin, 2018, p. 7). With its broad authority, it symbolized the centralization of China's cybersecurity governance, which demonstrated a more top-down governance approach that emphasized control over empowerment. Previously, in its efforts to boost the digital economy, the Chinese government "allowed" large technology companies such as Alibaba and Tencent to grow with relatively minimal regulatory constraints. As the capital capacity and influence of these companies grew, the Chinese government began to take systematic steps to centralize and restructure the formulation of cybersecurity policy. An editorial published on the Xinhua news agency website stated that the era of "barbaric" internet growth was over (Jiwei, 2018). Developments in several countries, including the US and China, where tighter controls and supervision had begun to be applied to technology companies, indicated a change in perspective on the internet. Innovation and growth of technology companies must be accompanied by supervision and corporate social responsibility. Internet, according to the editorial, had passed its "adolescence" and was now entering its "adulthood". One manifestation of this change in perspective was when, in July 2021, the CAC issued a regulation requiring any Chinese technology company wishing to make an overseas share offering to first obtain CAC approval.

Centralization of control and supervision was also carried out by ensuring government access to all national resources that could be mobilized for cybersecurity purposes. In 2016, for example, the Chinese government established the Cybersecurity Association of China (CSAC) as an industry association connecting various cyber stakeholders in China. This establishment aimed to bridge, organize, and mobilize all sectors of society to participate in developing China's cyber capacity. The members numbered more than 190 people, consisting of internet and network security companies, study institutions, and universities. Although officially intended as an industry association, CSAC remained under the control of CCP, ultimately contributing to the perpetuation of a top-down cybersecurity governance design (Fang, 2018, p. 457). Through information exchange and cooperation, it facilitated the strengthening of its members' innovation, study, and development capacities with the ultimate goal of accelerating China's achievement of cybersecurity technology independence. Furthermore, to study cooperation, CSAC members also played a role in promoting the formulation of cybersecurity and network security policies and strategies, as well as in building cooperation with the international community, specifically stakeholders from developing countries.

The change in cybersecurity policy initiated by President Xi Jinping also brought about changes in the cyber defense aspect. In 2015, the People's Liberation Army (PLA) formed the Strategic Support Force (SSF), which united all space, cyber, electronic, and psychological warfare capabilities in the PLA. The formation of the SSF significantly changed the organizational structure, doctrine, and culture. Information was now seen as a "strategic resource" in warfare. In addition, it could strengthen existing capabilities, but it also brought new vulnerabilities due to dependence on information systems. The formation of the SSF also showed a shift in China's defense doctrine from previously relying on asymmetric capabilities as the party was considered weaker in battle to symmetric warfare (Costello & McReynolds, 2018).

The SSF had 2 main roles, namely strategic information support and operations. The strategic information support role involved centralized collection and management of technical intelligence, strategic intelligence support for the theater command, supporting PLA power projection, providing strategic defense support in the space and nuclear domains, and supporting joint operations. Meanwhile, the strategic information operations role involved the coordinated deployment of space, cyber, and

electronic warfare capabilities to turn off enemy operational systems, specifically in the early stages of a conflict.

The SSF was subordinate to the Central Military Commission, which was part of the CCP and the administrative structure of the Chinese government. This consisted of 2 semi-independent sub-units, namely the Space Systems Department and the Network Systems Department. The Space Systems Department was formed from elements of the former General Armament Department. It was now responsible for nearly all aspects of PLA space operations, including space launch and support, telemetry, tracking and control, information support, and space warfare. The Network Systems Department, meanwhile, combined all units responsible for information operations in the PLA, including cyber warfare, electronic warfare, psychological warfare, and technical reconnaissance.

4. China's Approach to Global Cybersecurity Governance

Chinese government encouraged international cooperation and interaction to improve cybersecurity. Initially, international cooperation was more directed at opening access and absorbing advanced technology needed for the development of domestic cyber capabilities. Recently, as China's position in the international political constellation strengthened, international cooperation in the cyber field was directed more toward building mutual trust (confidential building measure). Furthermore, China has also utilized various international forums to promote cybersecurity governance norms and principles that were in line with its national interests.

President Xi Jinping placed cybersecurity in the context of great power competition (Austin, 2018, p. 6). The competition between great powers involved not only technological competition but also ideas and discourse. In a speech spoken at the World Internet Conference in Wuzhen in 2015, President Xi Jinping introduced the concept of "Internet sovereignty." According to Xi, the internet must be regulated by the same principles as other sectors in international relations. China emphasized that the principle of sovereignty that governed relations between countries also applied in cyberspace and was the basis for establishing rules in cyberspace. According to China, a country has jurisdiction over all cyberinfrastructure, resources, and activities that were located or occurred in its territory. Furthermore, each country must also have the right to formulate public policies in the field of information and communication technology according to the conditions of their respective countries and protect the interests of their citizens in cyberspace. Each country must also refrain from using cyber technology to interfere in domestic affairs and disrupt the political, economic, and social stability of other countries.

China's dissatisfaction with the status quo was also reflected in its approach to global cybersecurity governance. In its Strategy for International Cooperation in Cyberspace, for example, the Chinese government believed that the current system of Internet resource governance did not represent the wishes and interests of the majority of countries in the world. Every country, China argued, must participate in the fair management and distribution of Internet resources.

The Strategy for International Cooperation in Cyberspace document provided a comprehensive explanation of China's policies and positions on cyber issues in international relations (Strategy for International Cooperation in Cyberspace, n.d.). The document also formulated China's basic principles, strategic goals, and action plans in cyberspace.

- *Peace.* All countries must reject the Cold War mentality, zero-sum games, and double standards and strive for security based on respect for the security of others.

- *Sovereignty.* The principle of sovereignty in the UN Charter covered all aspects of relations between states, including in cyberspace.

- *Shared governance.* International cyberspace governance must use a multilateral approach. Every country had an equal right to participate in developing international rules in cyberspace.

- *Shared benefits.* Internet development must benefit all countries, and the international community must promote openness and cooperation in cyberspace.

In the White Paper on Military Strategy issued by the State Council in 2015, cyberspace, along with outer space, was considered to have become the most strategic area (command center) in the competition between major powers. The revolutionary changes in military technology (revolution in military affairs) and the defense transformation carried out by major powers were considered to be challenges to China's national interests. Furthermore, cyberspace was considered to be one of the new pillars of economic and social development. Therefore, it was considered to be a new domain of national security. As international competition in cyberspace intensifies, the potential threats to China's cyber infrastructure are also considered to be increasing. China was committed to accelerating the development of cyber power and strengthening the capabilities of cyber situational awareness, cyber defense, support for other activities in cyberspace, and international cooperation in cyberspace. The strategic objectives of this policy were to prevent the so-called "cyber crisis", ensure national network and information security, and safeguard national security and social stability.

5. China Cyber International Cooperation

The principle of “cyber sovereignty” introduced by President Xi Jinping in 2014 has become a key agenda pushed by China in several international cooperation forums. China was actively involved in the United Nations (UN) process on cybersecurity issues. This was done, among other things, by placing its representatives in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (UN GEE). Chinese representatives were also active in meetings of the Open Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG).

In addition to highlighting the issues of cyber attacks, cybercrime activities, and cyberterrorism, China also highlighted the actions of “a number of countries” that were considered to see cyberspace as a new battlefield. These countries were implementing a deterrence strategy by trying to build military alliances and develop rules of the game in cyberspace. According to China, it increased the risk of conflict in cyberspace. It endangered international peace and security, which tended to reject the application of the law of war and the principle of jus ad bellum in cyberspace. Countries, according to China, must not make cyberspace a new battlefield.

China also highlighted “some countries” that it said were politicizing technology and cybersecurity issues and restricting the movement of information and communications technology companies from other countries, therefore undermining the spirit of global cooperation and development. The country believed that the current uneven and unfair distribution of cyber resource management systems (the digital divide) posed a threat to the functioning of critical infrastructure.

China also used the UN forum to urge the international community to pay special attention to capacity-building efforts. Developed countries must increase technical and financial assistance to developing countries to improve their emergency response capabilities. Furthermore, China has encouraged all countries to strengthen international cooperation. In this regard, it emphasized the importance of building a multilateral, democratic, and transparent global cyber governance.

6. Bilateral and Trilateral Cooperation

Despite their differing views on global cybersecurity governance, the US and China have engaged in several cyber cooperation initiatives. Cybersecurity, for example, was one of the points of agreement reached during a meeting between President Xi Jinping and President Barack Obama in September 2015 (FACT SHEET: President Xi Jinping’s State Visit to the United States, 2015). Some of the points of agreement reached during the meeting included (1) China and the US agreed to provide prompt responses to requests for information and assistance related to malicious cyber activities, (2) China and the US agreed not to conduct or support cyber theft of intellectual property, including trade secrets and confidential business information, to gain a competitive advantage for companies or commercial sectors, (3) both countries committed to jointly identifying and promoting appropriate international norms to govern state behavior in cyberspace, and (4) China and the US agreed to establish a high-level dialogue mechanism to discuss cybercrime and related issues.

A series of ministerial meetings followed the Xi Jinping-Obama summit. In December 2016, China and the US held the third edition of the US-China High-Level Joint Dialogue on Cybercrime and Related Issues

(The Third US-China High-Level Joint Dialogue on Cybercrime and Related Issues, 2016). The meeting was attended by the US Prosecutor-General and the Minister of Homeland Security, the Chinese State Councilor, and the Minister of the Ministry of Public Security on the Chinese side. Several agreements reached at the meeting affirmed commitments made by China and the US at the Heads of State meeting a year earlier, including strengthening investigations of cybercrime and malicious cyber activities originating from China or the US and not conducting or supporting cyber theft of intellectual property. The 2 sides also discussed operational aspects of the agreement, including (1) strengthening network protection through measures such as sharing malicious IP addresses, malware samples, analytical products, and other network protection information, (2) continuing cooperation in the area of information sharing to combat the use of the internet for terrorism and criminal purposes, and (3) using hotline mechanisms to strengthen cooperation.

In October 2017, China and the US held the First US-China Law Enforcement and Cybersecurity Dialogue (LECD, 2017). The LECD was a ministerial-level meeting as a follow-up to the meeting between President Donald Trump and President Xi Jinping a few months earlier. Several commitments made at the previous meetings were reaffirmed at the LECD meeting. At this meeting, representatives from China and the US agreed to continue to pursue 5 points of cooperation, namely (1) providing a prompt response to requests for information and assistance related to cyber activities deemed detrimental, (2) both countries agreed not to conduct or support cyber theft of intellectual property, including confidential business and trade information, to gain competitive advantage for their respective companies or commercial sectors, (3) both countries jointly identified and promoted appropriate norms to regulate state behavior in cyberspace, (4) continuing high-level dialogue mechanisms to combat cybercrime and related issues, and, (5) strengthening law enforcement communication regarding cybersecurity incidents.

China also engaged with other Western countries, including US alliance partners, who tended to be libertarian in their approach to cybersecurity governance. The shared perceptions between the US and its alliance partners were reflected in the agenda of the meetings and agreements reached at the China-UK High-Level Security Dialogue held in June 2016 (China-UK High-Level Security Dialogue: Communiqué, 2016). At the meeting, China and the UK reached several points of agreement, including (1) both countries agreed not to conduct or support cyber theft of intellectual property, including business information and trade secrets, to gain competitive advantage for their respective companies or commercial sectors, (2) holding discussions on cybercrime issues through security dialogue mechanisms and annual working conferences on organized crime, to share information and experiences, (3) enhancing cooperation in responding to cybersecurity incidents and emergencies, where both countries agreed to provide a rapid response to requests for information and assistance regarding acts deemed dangerous, and (4) strengthening cooperation in the field of law enforcement to prevent and combat the use of the internet to incite, recruit, finance and plan terrorist activities.

In April 2017, China and Australia signed an agreement to strengthen cooperation in cybersecurity (Australia and China Agree to Cooperate on Cyber Security, 2017). In the agreement, both countries agreed not to conduct or support cyber theft of intellectual property, including confidential business and trade information, to gain a competitive advantage for their respective companies or commercial sectors. Furthermore, China and Australia also agreed to respect the norms identified in the UN-GGE reports and to establish a mechanism to discuss cybersecurity and cybercrime issues that had the potential to cause problems between the 2 countries. The Foreign Minister and Attorney General attended the Australia-China High-Level Security Dialogue from the Australian side, and the Head of the Chinese Communist Party's Central Commission for Political and Legal Affairs (CCPLA) from the Chinese side.

China's cyber cooperation with other authoritarian states took a different approach than its cooperation with Western countries. With these countries, China tended to emphasize joint efforts to promote the principle of cyber sovereignty in global cybersecurity governance. This was evident, for example, in China's interactions with Russia. In May 2015, during President Xi Jinping's visit to Russia, the Chinese and Russian Foreign Ministers signed an agreement on cooperation in the field of information security (Agreement on Cooperation in the Field of International Information Security) (On the Signing of the Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on Cooperation in the Field of Ensuring International Information Security, 2015). Both countries agreed that the main threats to information security were the use of information and communication technology to (1) commit violations of sovereignty, security, and territorial integrity, and threats to international peace, security, and strategic stability, (2) cause economic losses due to damage to

information infrastructure, (3) terrorist purposes, (4) violations and criminal acts, (5) interfere in the internal affairs of other countries, violation of public order, inciting ethnic, racial and religious hatred, spreading racist and xenophobic ideas that could incite hatred and discrimination, inciting violence and instability, disrupting the internal political stability and socio-economic situation of other countries, and (6) dissemination of information that endangered the socio-political and socio-economic systems, spiritual, moral and cultural environment of other countries.

China also paid attention to cyber cooperation with countries in the region. Together with South Korea and Japan, China held the first Trilateral Cyber Policy Consultation in Beijing in October 2014, the second in Seoul in October 2015, and the third in Tokyo in February 2017 (The 3rd Trilateral Cyber Policy Consultation, 2017). Through this senior official-level consultation forum, the governments of the 3 countries had the opportunity to exchange views on their respective countries' cyber strategies and policies. In this forum, China was represented by the Coordinator for Cyber Affairs, Ministry of Foreign Affairs.

In addition to the trilateral consultation forum at the senior official level, China, Japan, and South Korea also interacted through the China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response (5th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response Was Held in Korea, n.d.). The forum, attended by the CERTs of each country, aimed to review joint operations in handling cyber incidents and enhance cooperation to prevent cross-border incidents in the 3 countries. At the fifth meeting in 2017, delegates successfully mapped the capabilities of each country's CERT team and conducted a coordinated disclosure of vulnerabilities. Furthermore, CERT representatives from the 3 countries also better understood their respective roles in preventing and combating large-scale international cyber threats and agreed to provide support to each other.

China was also active in bilateral cooperation with Korea. In December 2016, China and Korea hosted the 2nd Korea-China Cybersecurity Forum (Korea, China Unite in Responding to Cyber Threats, Strengthening Industrial Cooperation, 2016). In addition to cooperation between state institutions, the forum was also used to strengthen partnerships between the private sectors of the 2 countries engaged in cybersecurity. In this forum, China was represented by senior officials from the Internet Security Management Directorate, Ministry of Industry and Information Technology, China Academy of Information and Communications Technology, and the National Computer Network Emergency Response Technical Team/China Coordination Center.

7. Conclusion

In conclusion, as China's cyber capabilities and influence in international politics strengthened, it had great potential to continue centralizing its domestic cybersecurity governance. Not only was it seen as a model capable of maintaining the legitimacy of the regime, but centralized governance was also considered quite effective in achieving China's interests in the contemporary cybersecurity sector, addressing cyber threats from within and outside the country, and promoting global cyber governance reform. Authoritarian cybersecurity policies were then considered capable of minimizing the risks or threats arising from activities in cyberspace.

China also rigorously promoted the norms and principles of state behavior in cyberspace that were in line with its preferences, specifically the principle of cyber sovereignty. Xi Jinping had placed cybersecurity in the context of major power competition. As a result, competition in this area was not only about technological competition. The effort to compete with ideas and discourse had become a major topic, specifically under China's dissatisfaction with the current Internet governance system, which was considered not to represent the wishes and interests of most countries in the world. With its cyber sovereignty narrative, China could continue to try to invite other countries to support the concept of cyber territorialization as an alternative to the current cyber governance.

As China's experience has shown, the opportunities and challenges presented by the development of information technology require a rapid response from the state. There needed to be a political commitment from the highest policymakers to place cybersecurity as part of national security. This could be started by standardizing the definition of the concept of national cybersecurity. Defining cyber threats, expected governance, policy directions, and other cybersecurity variables could help Indonesia to have a more integrated cybersecurity vision and strategy. Therefore, the state could move as an effective unit to create cybersecurity.

The adjustment of institutional structure carried out by China after 2014 also provided a lesson that simplifying institutional structure could strengthen coordination between institutions. In addition, it was undeniable that in complex cyber governance, there could be many challenges that had the potential to reduce the ability to maintain cybersecurity. In terms of resources, a country could not have adequate cyberinfrastructure in terms of quality and quantity, both physically and in terms of the lack of qualified human resources. In terms of politics, a country consisting of a complex system of power and control could not be free from the presence of bureaucratic institutions competing for influence and autonomy. Based on China's experience, these problems could be overcome with clear direction and political commitment from the highest decision-makers to change the situation. With clear direction and commitment, the time needed for the restructuring process was also relatively fast.

China's cyber governance strategy also showed that strong public-private partnerships were a prerequisite for the country to maximize the potential of information and communications technology while minimizing the negative impacts and cybersecurity threats that came with it. Ensuring that the government had access to all national resources that could be mobilized for cybersecurity purposes, including the potential offered by the private sector, was a must. The country could maximize the potential of the private sector by facilitating its involvement in cybersecurity industry associations and by creating policies that could expand companies' access to the global market. After that, the country found it easier to monitor the cyber responsibility of companies and ensured that their activities complied with applicable cybersecurity laws and regulations.

China was not only able to build a capable cyber power base but also managed it little by little to produce the desired security conditions. In this case, it reflected the importance of measuring national cybersecurity from the perspective of results, not just resources (cyber power). This meant that a country could not simply be proud of the cyberinfrastructure it had but must be able to ensure that the resources (cyber power) it had could produce the desired conditions (cybersecurity).

References

5th China-Japan-Korea CSIRT Annual Meeting for Cybersecurity Incident Response was held in Korea. (n.d.). CNCERT/CC. Retrieved October 20, 2021, from https://www.cert.org.cn/publish/english/55/2017/20170921100705257184781/20170921100705257184781_.html

Akyesilmen, N. (2018), Cyber good Governance: A new Challenge in International Power Politics?" Cyberpolitik Journal 3(6). www.cyberpolitikjournal.org.

Ang, B. (2021). Singapore: A leading actor in ASEAN cybersecurity. Dalam Romaniuk, S. N. & Manjikian, M (ed) Routledge Companion to Global Cyber-security Strategy. Oxon: Routledge.

Areng, L. (2014). "Lilliputian States in Digital Affairs and Cyber Security." Tallinn Paper No. 4. CCDCOE, Tallinn, Estonia. https://ccdcoe.org/uploads/2018/10/TP_04.pdf.

Austin, G. (2016). Mapping and Evaluating China's Cyber Power (Policy Paper Series). Lau China Institute.

Austin, G. (2018). Cybersecurity in China: The Next Wave. Springer International Publishing. https://doi.org/10.1007/978-3-319-68436-9.

Australia and China Agree to Cooperate on Cyber Security. (2017, April 24). Department of the Prime Minister and Cabinet. https://pmtranscripts.pmc.gov.au/release/transcript- 40910.

Baram, G. (2017). "Israeli Defense in the Age of Cyber War." Middle East Quarterly, 24(1):1– 10). www.meforum.org/middle-east-quarterly/pdfs/6399.pdf.

Brenner, Joel., & Lindsay, Jon R. (2015). Correspondence: Debating the Chinese Cyber Threat. International Security 40:1, 191-195

Brown, G., Carlye, M., Salmeron, J. & Wood, K. (2006). "Defending Critical Infrastructure," Interfaces, 36(6): 530–544.

Buzan, B. & Hansen, L. (2009). The Evolution of International Security Studies. Cambridge: Cambridge University Press.

Cavelty, M. D. & Egloff, F. (2019). "The Politics of Cybersecurity: Balancing Different Roles of the States." St. Antony's International Review 15(1), 37-57.

Chang, Evelyn. (2021). China says it now has nearly 1 billion internet users. CNBC. https://www.cnbc.com/2021/02/04/china-says-it-now-has-nearly-1-billion-internet- users.html.

Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: Balancing national security, geopolitical, and development priorities. Journal of Cyber Policy, 3(3), 306– 326. https://doi.org/10.1080/23738871.2018.1556720.

China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. (n.d.). Retrieved October 20, 2021, from chrome- extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Funoda-web.s3.amazonaws.com%2Fwpcontent%2Fuploads%2F2019%2F09%2Fchina-submissions-oewg-en.pdf&clen=109616&chunk=true.

China-UK High Level Security Dialogue: Communique. (2016, June 13). GOV.UK. https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue- official-statement/china-uk-high-level-security-dialogue-communique.

Chouchri, Nazli., Madnick, Stuart., & Priscilla Koepke. (2017). Institutions for Cyber Security: International Responses and Data Sharing Initiatives. Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management, Massachusetts Institute of Technology, DOI: 10.1080/02681102.2013.836699.

Costello, J., & McReynolds, J. (2018). China's Strategic Support Force: A Force for a New Era (No. 13; China Strategic Perspectives, p. 84). Institute for National Strategic Studies.

Craigen, D., Diakun-Thibault, N., Purse, R. (2014). "Defining Cybersecurity." Technology Innovation Management Review 4(10), 13-21.

Creemers, Roger. (2019). The International and Foreign Policy Impact of China's Artificial Intelligence and Big-Data Strategies. Dalam Artificial Intelligence, China, Russia, and the Global Order. Air University Press.

Cristiano, F. (2021). Israel: Cyber defense and security as national trademarks of international legitimacy. Dalam Romaniuk, S. N. & Manjikian, M (ed) Routledge Companion to Global Cyber-security Strategy. Oxon: Routledge.

Cuihong, C. (2018). China and Global Cyber governance: Main Principles and Debates. Asian Perspective 42(4), 647-662.

de Bossey, Cgateay. (2005). Report of the Working Group on Internet Governance, Source: http://www.wgig.org/docs/WGIGREPORT.pdf.

DeVore, M. R. & Lee, S. (2017). "APT (Advanced Persistent Threat)s and Influence: Cyber Weapons and the Changing Calculus of Conflict," The Journal of East Asian Affairs, 31(1): 39–64. Retrieved from www.jstor.org/stable/pdf/44321272.pdf.

Dhillon, G. (2007). Principles of Information Systems Security: Text and Cases. New York: John Wiley & Sons.

Eriksson, J. and Giacomello, G. (2006). 'The Information Revolution, Security and International Relations: (IR)relevant Theory?' International Political Science Review, 27(3): 221–44.

FACT SHEET: President Xi Jinping's State Visit to the United States. (2015, September 25). The White House. https://obamawhitehouse.archives.gov/the-press- office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Fallows, D. (2008). Most Chinese Say They Approve of Government Internet Control. Pew Internet & American Life Project.

Fang, B. (2018). Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace. Springer.

Fei, Gao. (2011). China's Cybersecurity Challenges and Foreign Policy. Georgetown Journal of International Affairs, International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity. 185-190.

First U.S.-China Law Enforcement and Cybersecurity Dialogue. (2017, October 6). Department of Homeland Security. https://www.dhs.gov/news/2017/10/06/first-us- china-law-enforcement-and-cybersecurity-dialogue

Fjäder, C. O. (2016). National security in a hyper-connected world: global interdependence and national security. Dalam Masys, A. J. (ed) Exploring the security landscape: non- traditional security challenges. Springer.

Full text of "National Cyberspace Security Strategy." (2016, December 27). Office of the Central Cyberspace Affairs Commission. http://www.cac.gov.cn/2016- 12/27/c_1120195926.htm

Geiger, A. W. (2018). "How Americans Have Viewed Government Surveillance and Privacy since the Snowden Leaks," Pew Research. www.pewresearch.org/fact- tank/2018/06/04/how-americanshave-viewed-government-surveillance-and-privacy- since-snowden-leaks.

Grauman, B. (2012). Cyber-Security: The Vexed Question of Global Rules. An Independent Report on Cyber Preparedness around the World. Brussels: Security & Defence Agenda (SDA) and McAfee Inc. (Security & Defence Agenda).

Hansen, L. & Nissenbaum, H. (2009). "Digital Disaster, Cyber Security, and the Copenhagen School," International Studies Quarterly 53, 1155–1175.

Inkster, Nigel. (2015). Evolution of the Chinese Internet: Freedom and Control. Adelphi Series, 55: 456, 19-150. https://doi.org/10.1080/19445571.2015.1181441.

International Strategy of Cooperation on Cyberspace. (n.d.). Ministry of Foreign Affairs of the People's Republic of China. Retrieved October 22, 2021, from https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml

International Telecommunication Union. (2017). Global Cybersecurity Index 2017. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

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

Jiwei, L. (2018, April 25). The era of barbaric growth on the Internet is over. XINHUANET.Com. http://www.xinhuanet.com/tech/2018-04/25/c_1122740358.htm

Kementerian Luar Negeri dan Administrasi Ruang Siber China. (2017). International Cyberspace Cooperation Strategy. CD/2092. https://undocs.org/CD/2092

Korea, China join forces in responding to cyber threats, strengthening industry cooperation. (2016, December 21). Embassy of the Republic of Korea in the United Kingdom of Great Britain and Northern Ireland and Permanent Mission to the International Maritime Organization. https://overseas.mofa.go.kr/gb-en/brd/m_8349/view.do?seq=749192

Kurbaija, Jovan. (2016). An Introduction to Internet Governance, 7th Edition. Geneva: DiploFoundation.

Kurbalija, J. (2016). An Introduction to Internet Governance. DiploFoundation.

Li, J. (2021, August 23). How China's top internet regulator became Chinese tech giants' worst enemy. QUARTZ. https://qz.com/2039292/how-did-chinas-top-internet-regulator- become-so-powerful/

Lindsay, Jon R. (2015). The Impact of China on Cybersecurity: Fiction and Frcition. International Security 39:3, 7-47

Manjikian, Mary. (2021). The United States: A Declining Hegemon in Cyberspace? Dalam Romaniuk, S.N & Manjikian, M (ed). Routledge Companion to Global Cyber-security Strategy. Oxon: Routledge.

McKune, S. & Ahmed, S. (2018). "The Contestation and Shaping of Cyber Norms through China's Internet Sovereignty Agenda," International Journal of Communication, 12, 3835-3855.

McKune, S. (2015, September 28). An analysis of the International Code of Conduct for Information Security. Toronto, Canada: Citizen Lab. https://citizenlab.ca/2015/09/international-code-of-conduct/

Miao, W., & Lei, W. (2016). Policy review: The Cyberspace Administration of China. Global Media and Communication, 12(3), 337–340. https://doi.org/10.1177/1742766516680879

Miao, W., Jiang, M., & Pang, Y. (2021). Historicizing Internet Regulation in China: A Meta- Analysis of Chinese Internet Policies (1994–2017). International Journal of Communication, 15, 2003–2026.

Mueller, M. (2010). Networks and States: The Global Politics of Internet Governance. MIT Press.

Mueller, M. (2017). Will the Internet Fragment? Sovereignty, Globalization and Cyberspace. London: Polity.

National Computer Network Emergency Response Technical Team/Coordination Center of China. (n.d.). CNCERT/CC. Retrieved October 20, 2021, from https://www.cert.org.cn/publish/english/index.html

Newman, K. L. (2000). Organizational transformation during institutional upheaval. The Academy of Management Review, 25(3), 602–619.

On the signing of an Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on cooperation in the field of ensuring international information security. (2015, May 8). Ministry of Foreign Affairs of the Russian Federation. https://www.mid.ru/ru/maps/cn/-/asset_publisher/WhKWb5DVBqKA/content/id/1257295

Panda, A. (2014, March 4). Xi Jinping: China Should Become a "Cyber Power." The Diplomat. https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/

PLA Cyberspace Strategic Intelligence Research Center founded. (2014, July 1).

Chinanews.Com. http://www.ecns.cn/military/2014/07-01/121758.shtml

Ran, J. (2017, March 15). American unrest proves China got the Internet right. Foreign Policy. https://foreignpolicy.com/2017/03/15/american-unrest-proves-china-got-the-internet- rightbeijing-great-firewall-censorship-trump/

Rapoza, K. (2013, June 22). U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press. Forbes. https://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked- china-universities-mobile-phones-snowden-tells-china-press/?sh=666824065340

Robinson, N. & Hardy, A. (2021). Estonia: From the "Bronze Night" to cybersecurity pioneers. Dalam Romaniuk, S. N. & Manjikian, M (ed) Routledge Companion to Global Cyber- security Strategy. Oxon: Routledge.

Stadnik, Ilona. (2021). Seeking a New Order for Global Cybersecurity: The Russian Approach to Cyber-sovereignty. Dalam Romaniuk, S.N & Manjikian, M (ed). Routledge Companion to Global Cyber-security Strategy. Oxon: Routledge.

Statista. (2021). Number of internet users in China from 2015 to 2020 with a forecast until 2026. https://www.statista.com/statistics/278417/number-of-internet-users-in-china/.

Stevens, Tim. (2021). United Kingdom: Pragmatism and Adaptability in the Cyber Realm. Dalam Romaniuk, S.N & Manjikian, M (ed). Routledge Companion to Global Cyber- security Strategy. Oxon: Routledge.

Tabansky, L. & Ben-Israel, I. (2015). Cyber Security in Israel. New York: Springer.

Tabansky, L. (2013). Cyberdefense Policy of Israel: Evolving Threats and Responses. Chair de Cyberdefense et Cybersecurite.

The 3rd Trilateral Cyber Policy Consultation. (2017, February 8). Ministry of Foreign Affairs of Japan. https://www.mofa.go.jp/press/release/press4e_001471.html

Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues. (2016, December 8). Department of Homeland Security. https://www.dhs.gov/news/2016/12/08/third-us-china-high-level-joint-dialogue-cybercrime-and-related-issues under-donald-trump.

Wickett, X., Smith, J., & Smart, C. "America's International Role under Donald Trump." Chatham House Reports. January 18, 2017.

https://www.chathamhouse.org/publication/americas-internationalrole-

World Bank. (2021). Individuals Using the Internet (% of Population). https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2019&start=1960&view=chart.

Xi wants China to be "cyber power." (2014, March 1). DefenceTalk.Com. https://www.defencetalk.com/xi-wants-china-to-be-cyber-power-58886/

Ye, Z. & Zhao, B. (2014). Thoughts on Internet sovereignty, Internet borders, and national network defense. China Information Security.

Zeng, J. (2015). The Chinese Communist Party's Capacity to Rule: Ideology, Legitimacy and Party Cohesion. Palgrave Macmillan.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." Politics & Policy, 45(3), 432–464. https://doi.org/10.1111/polp.12202.