Institute of Chinese Studies
ICS
中国研究所 DELHI

OCCASIONAL PAPER

No. 55

August 2020

China's Cyber Governance: Between Domestic Compulsions and National Security

Mrittika Guha Sarkar

ICS OCCASIONAL PAPER NO. 55

China's Cyber Governance: Between Domestic Compulsions and National Security
Authors: Mrittika Guha Sarkar

First published in 2020

Institute of Chinese Studies
8/17 Sri Ram Road, Civil Lines
Delhi 110 054, INDIA
Ph.: +91-11-23938202; Fax: +91-11-23830728
Email: info@icsin.org
Website: www.icsin.org

ABOUT THE AUTHOR

Mrittika Guha Sarkar is a research scholar at the Centre for East Asian Studies, School of International Studies, Jawaharlal Nehru University (JNU), New Delhi. Her research areas are India-China relations, East Asia's geopolitics and security studies focusing on regional affairs of China, Japan and Korea. She writes for several journals, newspapers and magazines such as Business Today, East Asia Military Monitor, World Focus, Defense and Security Alert (DSA) and The Pioneer. Her recent publications include "The Big Picture: US Ban on Huawei", "Shifting Sino-US Military Relations", "Changing Trends between India and Nepal", "Dalai Lama Holding Tongue on Doklam?" and "India-Vietnam Outreach: Strengthened Ties". She has been a project assistant and an intern with the East Asia Centre at the Institute for Defence Studies and Analyses (IDSA), New Delhi. She is also an editorial assistant for Routledge Studies on Think Asia.

Contact: mrittika11@gmail.com

Traditional Cultural Ideas and Symbols, and Possibilities of Discursive Legitimacy in Contemporary China

Abstract

Since the advent of the internet era, different countries have adopted diverse approaches for the regulation and governance of the cyberspace. These approaches have often been divergent as well as contradictory to each other, causing an unresolved debate for an ideal framework for cyber laws. The year 2016 witnessed a series of developments in China's cyber governance, particularly with the enactment of the cybersecurity law. China has been propagating its concept of "cyber sovereignty," extending its influence in the fifth dimension and providing a competitive alternative to the dominant notions of "open internet." It has viewed the internet space through the lens of Neo-Realism, as an unruly space where the technologically advanced can dominate. As a result, China's cybersecurity law targets an overhaul of the internet, aiming to secure its cyberspace, reducing dependence on foreign technology and acquiring the ability to surveillance and control information online. While it's technological developments are resulting in economic growth, advances in surveillance, data mining, as well as artificial intelligence, have been having significant implications on society. At the same time, while many countries have been in synergy with the Chinese approach of internet governance, several countries, including the United States (US) have accused China of cyber espionage and targeting sensitive data. In this context, this paper aims to examine China's concept of cyber sovereignty through theoretical underpinnings of national security, economic development, and societal interests. It further purports to examine the implications of China's cyber sovereignty in domestic as well as the global arena, in the backdrop of a growing US-China cyber conflict. Lastly, it aims to highlight the possible challenges to China's cyber governance, having possible repercussions for the legitimacy of the leadership in the post-COVID-19 period.

Key Words: Cybersecurity, Internet governance, Cyber sovereignty, US-China relations, China, USA

Introduction

The Cyberspace in recent years has evolved into a critical arena which cuts through all aspects of human life. It has its dependencies varying from individuals to groups, corporations, banks, the critical infrastructures, and more; encompassing the basic functionalities of a nation-state. It has also been playing a crucial role in the fields of national and international politics, especially in regard to the debates on cyber sovereignty, cyber governance, and cybersecurity. China, as a latecomer to the cyber domain, is not devoid of these debates and has instead advocated for its version of cyberspace and governance. Contrary to the arguably dominant vision of free and open cyberspace, China has promulgated an authoritarian space where governance factorizes regulations and restrictions. This form of governance stems from China's concept of cyber sovereignty, which signifies that it will choose a development intensive path that would cater to its interests, formulate laws according to its national security considerations and condemn any external intrusions to its cyber governance. While doing so, it would aim to acquire sufficient cyber capabilities to ensure technological independence and overall self-sufficiency in the backdrop of a worsening external environment. Such an approach towards cyber governance, has, however, witnessed divergences and frictions from countries such as the US, leading to debates and deliberations regarding the 'correct form' of cyber governance.

In this context, this paper aims to examine China's cyber governance and its vision of the cyber domain. The article analyzes how its national security and international concerns have increasingly shaped China's cyber sovereignty. While doing so, the paper examines the implications of China's cyber governance on its domestic as well as the external environment. Finally, the paper draws on the hypotheses that China's cyber governance model is a unique juxtaposition of an authoritarian society controlling the cyberspace through regulations and restrictions; and at the same time, emphasizing on technological advancement and a strengthened internet. China's cyber governance model diverges from the dominant model of governance, resulting in the creation of frictions with countries endorsing an arguably free and open cyber domain with uncontrolled information exchange.

The Cyberspace in the Communist Party of China (CPC)

The profound impact of the cyberspace on all aspects of statecraft and governance, including the areas of economic, military, diplomacy, and technology, stands undebated. Xi Jinping was one of the first Chinese leaders to acknowledge and comprehend its unprecedented development and advocate 'China as a Cyber Power.'[1] However, it was in the post-Mao era in China, especially under Deng Xiaoping that China was encouraged to develop in the field of science and technology to ensure China's economic progress. These pushed China closer to modernization, with science and technology as the pillars of socio-economic development. Subsequently, Jiang Zemin promulgated the development and utilization of IT in all areas of China's social and economic development.[2] He emphasized on the importance of IT and the utilization of Information and Communication Technology (ICT) to bring about a leapfrog development in China's modernization.[3] However, the first mention of the term 'cyber' was by Hu Jintao in his report of the 17th Party Congress in 2007.[4] This was mainly after a series of Denial of Service (DoS) attacks on Estonia which targeted its parliament, government ministries, major banks, media that lead Estonia to a complete standstill.[5] Subsequently, Hu Jintao acknowledged the growing importance of the cyber domain, not only as a boon but also as a potential threat. After these attacks, Hu Jintao decided to regulate the cyberspace and maintain a correct internet environment. Successively, he envisioned building China into an 'innovation-oriented country' to create a self-sufficient society that would progress on the path of socialist modernization.[6] Thus, Hu Jintao during the 18th Party Congress emphasized on the important maritime, space, and cybersecurity areas, which were to shape China's policies and priorities focussing on the cyber domain in the coming years. On the same lines, Xi Jinping today acknowledges the innovation-driven development strategy and considers it as one of the most significant instruments that can take China out of the 'middle-income trap.'[7] For Xi Jinping, a modernized economy with technological strength contributes to the country's Comprehensive National

Power (CNP) and its international stature. Hence, China has been increasingly integrating its economy with technology. One of the most excellent examples has been the development of the Belt and Road Initiative (BRI) which has been expanded to include science and technology; focus on building a digital and smart connectivity infrastructure; strengthen cyberspace and aerospace; develop common technology standards; and improve the efficiency of regulating systems amongst the BRI countries through the Digital Silk Road (DSR).[8] The DSR, aiming to enhance the connectivity concept of the BRI, was introduced as the "information Silk Road" in China's White paper of 2015, jointly issued by the National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China.[9] However, in the backdrop of China's authoritarian management of the cyber domain and its goal to attain the "Chinese Dream" of national rejuvenation[10], the DSR can be argued as a vehicle for China's control over the global internet and a masterplan to deploy its regulatory model along with the BRI countries. This argument could be better proven by comprehending China's cyber management under Xi Jinping.[11]

Xi, in the 19th Party Congress, had promoted bolstered means of communication and extensive use of the internet for party work. Noteworthy are the strategic imperatives of this development. Greater use of IT and internet within the party and for party work has been considerably enhancing the CPC's legitimacy. By enabling it to have a more prominent means of communication within, it also allows the party to communicate its ideology in an enhanced way with a broader range of masses. Importantly, Xi Jinping's speech signified his aim to provide the public with the correct tone of communication and clean cyberspace by stating:

> *We will maintain the right tone in public communication, give priority to improving means of communication and to creating new ones, and strengthen the penetration, guidance, influence, and credibility of the media. We will provide more and better online content and put in place a system for integrated internet management to ensure a clean cyberspace. We will implement the system of responsibility for ideological work, and further consolidate our positions and improve management in this field. We will distinguish between matters of political principle, issues of*

> *understanding and thinking, and academic viewpoints, but we must oppose and resist various erroneous views with a clear stand.*[12]

This statement expressed the core principles of China's vision of cyber governance. The statement reiterated CPC's idea of regulating the cyberspace according to its own ideology and interests. Xi's speech propounded that the party would decide what the population of China should and should not view and oppose any stand, which it feels is erroneous. The party would do so by upholding stringent censorship on any content it deems unacceptable to be viewed.[13] This step is supported by the law of the government of China and would account for strict reproach if not followed.

Internet in China is prominently controlled by the Cyberspace Administration of China (also known as the Office of the Central Leading Group for Cyber Affairs) founded in 2011 and currently led by Xi Jinping. Other stakeholders include the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS). Importantly, the former agency runs parallel to the party propaganda system and the government's information office system, headed by the Central Propaganda Department and the State Council Information Office, respectively. The information management is legally institutionalised by the "Administrative Measures on Internet Information Services", issued by the State Council in 2000, and the "Administrative Provisions of Internet News Information Services", issued by the State Council and the Ministry of Information Industry in 2005. The former sets out legal conditions for the websites to operate, including registration and licensing. The latter establishes the system for online news publication, dividing the online news agencies into three categories: those run by news entities, those run by non-news entities, and those established by news entities to carry already-published content.[14] There is a significant amount of state control on online news publication as a medium of surveillance and control. In this regard, state-run news agencies such as Xinhua and People's Daily are allowed to produce news, while the rest are enabled only to reprint; as a mode of occupation of the cyberspace by the state.

Most importantly, China has devised the Great Firewall, a combination of legal actions and technologies to regulate the internet through censorship.[15] In addition to this, in 2015 China under Xi Jinping launched the Great Cannon, which unlike the Great Firewall could act as an offensive tool by executing Denial of Service (DoS attacks) which would divert internet traffic which flows through it to overload targeted websites, leading it to go down.[16] The above restate the core principles of cyber governance by the CPC, which emphasis on controlling the cyber domain according to its ideologies and a will to ensure complete power over China's territory and people. However, what is intriguing about the governance in China is the relationship between authoritarianism and technological development. An explanation for this is placed in the capabilities of the CPC to adapt to the rapidly changing environment of the cyberspace; at the same time, sustain its control over the domain.

In this context, akin to the Arab Spring, advancement in online expression has strengthened regime supporters as much as the critics. This has occurred due to the party's attractive online and offline propaganda, as well as the growing online interaction between the regime supporters and the masses, in turn expanding the influence of the party.[17] For instance, the Chinese government has initiated innovative propaganda tactics such as the *fifty-cent army* by hiring internet commentators to manipulate public opinion. By utilizing the fifty-centers, the CPC has been able to sustain its legitimacy and consolidate power over the people of China by enhancing the government's PR effectiveness.[18] If anything, this kind of strategy helps China to better cope with the challenges of possible fragmentation of the Chinese society by questioning the credibility of the CPC. Thus, China is growing with an authoritarian government, coexisting with an empowered scientific and industrial space.

However, irrespective of its path-breaking research and development in the technological area such as Artificial Intelligence (AI), telecommunication giants of Huawei, Alibaba, ZTE, Tencent, and more which are increasingly enhancing their global footprint,[19] China and its 800 million internet users[20] are not immune to cyber threats and cyber-attacks. Its principles of cyber governance are as much built on a defensive strategy securing its cyberspace with strict regulations and codes of conduct, as on an offensive strategy to promote technological innovation and development and ensure national security. In this regard, it is imperative to understand China's principles of cyber governance and its concept of cyber sovereignty in the context of conventional and non-conventional threats it faces in the domestic as well as in the international sphere.

China's Threat Perceptions and Cyber Governance

China's concept of cyber sovereignty remains shaped by concerns regarding not just cybersecurity but also its national security. It must be noted that threats in the cyber era are not necessarily restricted to traditional means through land, sea, or air. It has become much more unconventional. The fear is that a cyber-attack (cyber terrorism, cyber espionage, cybercrimes) by a state or even a third party on China's critical infrastructures could handicap the country and cause as much destruction as any traditional military attack. China understands the severity of the unconventional threat and has not wasted any time linking its national security with cybersecurity.

Xi Jinping, in his speech in the first session of the Central Leading Group for Cyberspace affairs in 2014, reiterated the importance of internet control as the key to stability in China. He propounded:

> *'No cybersecurity, no national security. No informatization, no modernization. Only by using security to guarantee development and using development to promote security, can long-term peace and order be realized'.*[21]

Xi's speech denotes the significance for China to strengthen its grip over the internet to meet its core national goals. One of the major drivers for China's emphases on internet control is the necessity to have the ability to attain and maintain its core strategic interests. These include sustaining CPC's power and ensuring the survival of Xi Jinping's thought on 'Socialism with Chinese Characteristics for a New Era'; Sustaining and enhancing economic growth to strengthen China's CNP,[22] legitimising the CPC's authority, fulfilling China's objectives of global technological dominance and enabling it to escape the 'middle-income trap'; Maintaining national unity by defending territory and reinforcing territorial claims in Xinjiang, Taiwan and the India-China border; Preventing secessionism, separatism and independence activities in

Xinjiang, Tibet, Taiwan, Inner Mongolia and Hong Kong; Maintaining peaceful and stable relations with neighbouring countries and upholding its neighbourhood policy; Reasserting the maritime claims in the ECS and the SCS; Pushing back the influence of the United States in the regional domain, particularly against the backdrop of Washington's security alliances with South Korea and Japan; and the former's relationship with Taiwan – a hindrance to Beijing's 'One China Policy'; and Reshaping the global order so that Chinese values and interests are accepted universally.[23]

Further, it is important for China to defend its people and territory from the three evils- terrorism, extremism, and separatism.[24] China has time and again emphasized on sovereignty and territorial integrity. Its defence white papers have expressed commitment in combating the three evils. The evil of terrorism is no more restricted to land, water, or air; but has also moved into the cyberspace and has been used as a safe haven for planning terrorist attacks. This space enables terrorists to easily find and target political, social, or religious objectives.[25] China is also not been devoid of the same and experienced such attacks during the Yunnan Kunming Railway Station terrorist attack and the Urumqi South railway station terrorist attack. Further, China has very cautiously and carefully restricted several social networking sites, forums, chat rooms, and other social interactive platforms to prevent erroneous thoughts of separatism and extremism to corrupt the communist ideology and threaten the security of China.

In view of China's threat perceptions, Xi Jinping, under his administration, has acknowledged the hazards of the internet and pushed for tighter controls and surveillance on the information accessible to citizens. In retrospect, Xi viewed cyberspace as a medium for the Arab Spring and pro-democracy agitations across North Africa and West Asia in 2010-11, comprehending its possible impacts on the regime stability in China. This holds greater significance in view of the strategically critical security concerns China faces today, regarding it as a crucial factor in shaping its cyber governance.

Defensive Strategies against Cyber Attacks

The Chinese leaders view cyberspace through three primary lenses of national security and domestic stability, preserving the rule of the CPC and facilitating economic growth.[26] Article 35 of the Constitution allows the people of China the fundamental freedoms of speech, of the press, of association, demonstration and procession.[27] However, subsequent articles in the Constitution condemn citizens who engage in any activities which are deemed erroneous towards the government. This similarly is applicable for cyberspace where any content which is directed against the government or questions the CPC rule is condemned, and becomes a matter of national security.[28]In hindsight, China has been controlling public information since the 1950s. Further, post-Tiananmen Square 'incident', tighter controls over the masses were initiated. The same can be applied to the internet governance in China where it exercised stringent controls over the content flow to ensure the preservation of the state security and the public order; socialist and communist ideals; and the legitimacy of the CPC. Entering cyberspace relatively later than many advanced countries, it acknowledged the openness and limitlessness of the cyberspace. Accordingly, the CPC also sensed the perils of the space for its control over the masses. Thus, China throughout the later decades of the 20th century and till the current times has been maneuvering between the need for advanced technology for higher economic growth and the prevention of polluting the state ideals through external influences. The correct balance between both has been a defensive strategy to prevent cyber-attacks in China.

China's Cyber Governance and Cyber Sovereignty

The Cyberspace, for the CPC, remains an essential ingredient for the functionality of China's economy, polity as well as society. It has become the backbone of research and development in the country. The Cyberspace has also become factored with censorship against content on the internet, which goes against China's Constitution. In this regard, cyber sovereignty has remained the foundation for China's cyber policies and diplomacy. A milestone document reiterating this fact was the White Paper on the Internet by China in 2010 published by the State Council.[29] The document stated:

> *'the Internet of various countries belongs to different sovereignties, which makes it necessary to strengthen international exchanges and cooperation in this field. (...) China supports the establishment of an authoritative and just international Internet administration organization under the UN system through democratic procedures on a worldwide scale'.*[30]

Successively, the White Paper in 2013 on Diplomacy stressed on the concept of territorial sovereignty and expressed China's opposition towards interference by any country in its internal affairs.[31] The paper talked about the cyber-attacks China experienced the year before and urged the international community to strengthen its cooperation in ensuring a peaceful, secure, open, and cooperative environment.[32] However, the element of ambivalence is manifested in China's document on Cybersecurity Law passed in 2016 and implemented in June 2017, which linked distinct sovereignties to different countries.[33] According to the document, every country has different sovereignty, and irrespective of cyberspace being a global arena, how a country should be governed should be subjected to its jurisdiction.

Hence, according to these documents, China recognizes the open and democratic procedures of the cyber world and has no qualms administering according to the UN system. However, it believes in the concept of freedom to adjudicate its cyberspace according to its own will and apply rules and regulations wherever it deems necessary. Further, China's 'International Strategy of Cooperation on Cyber Space' states:

> *.... No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone, or support cyber activities that undermine other countries' national security.*[34]

This also reiterates the imperatives of the cyberspace to not just China's economy and the developmental sector but also for its strategic affairs. Through this statement, China advocates its beliefs towards any forms of interference in China's internal affairs as an act of cyber hegemony and a threat to national security. Cyber sovereignty, hence, becomes a defence strategy for China to block any content detrimental to China and its national security.

Interestingly, in the backdrop of the above, China in 2017 introduced its National Intelligence Law which unraveled the deep and profound influence of the CPC in the Chinese telecommunications and other Chinese owned and operated companies around the world. This law was created to provide guidelines for ensuring network security, protecting the rights and interests of the people, and promote the secure and stable development of technology.[35] However, while doing so, it requires the data to be stored in China and obligates Chinese companies to 'support, assist and co-operate with the state intelligence-gathering work', reiterating the possibility of national security information to be passing through the CCP as a legal mandate.' This, if anything, risks the possibility of leaving the intellectual property and private information vulnerable to government abuse while providing the government with the legal right to control information by forcing domestic, as well as foreign companies to comply with investigative measures under the garbs of national security.[36]

Military Defences

China has recognised the existence of cyber-attacks, its potential, and has been preparing the People's Liberation Army (PLA) to deter them. It is currently strengthening the PLA Strategic Support Force (PLASSF) through an approach of 'no attack first.'[37] Subsequently, its network systems department has combined the technical reconnaissance bureaus (TRBs) from the former Third Department (3PLA) of the General Staff Department (GSD) responsible for intelligence services. This has been done to centrally control the intelligence services, which account for a significant role in China's defensive and deterrent strategies. Further, the centralized command and control systems using integrated information and firepower can aggrandize China's military cyber power.[38] However, for PLA, coordinating information across the various units as well as synchronizing warfare capabilities remains the primary test, especially under the newly formed theatre commands. Moreover, the Central Military–Civil Fusion Development Commission's formalized Cyberspace Security Military–Civil Fusion Innovation Centre, which is being led by Xi Jinping himself, is aiming at national cyber defences.[39] In this regard, the capital of China, Beijing, could also host cyber militias for China's cybersecurity.[40] This reverberates a strategic and military aspect in its cyber governance.

Implications of China's Cyber Sovereignty on Society

China, as its recent policies and law frameworks suggest, is taking an authoritarian approach to establish a state-centric and all-encompassing control of internet content accessible to its population. Further, its science and the technology sector is developing under China's nationalist approach.[41] While these policies have been highly successful in an economic forum, these approaches are not without considerable costs. *Firstly*, as per the United Nations, extensive control over the internet or forbidding access to the internet is a violation of human rights.[42] In this context, it is essential to note that China itself promotes cooperation with the international community and establishment for a just internet administrative organization under the UN system.[43] Thus, this policy by China has not just received extensive international criticisms but has also witnessed domestic despair.[44]

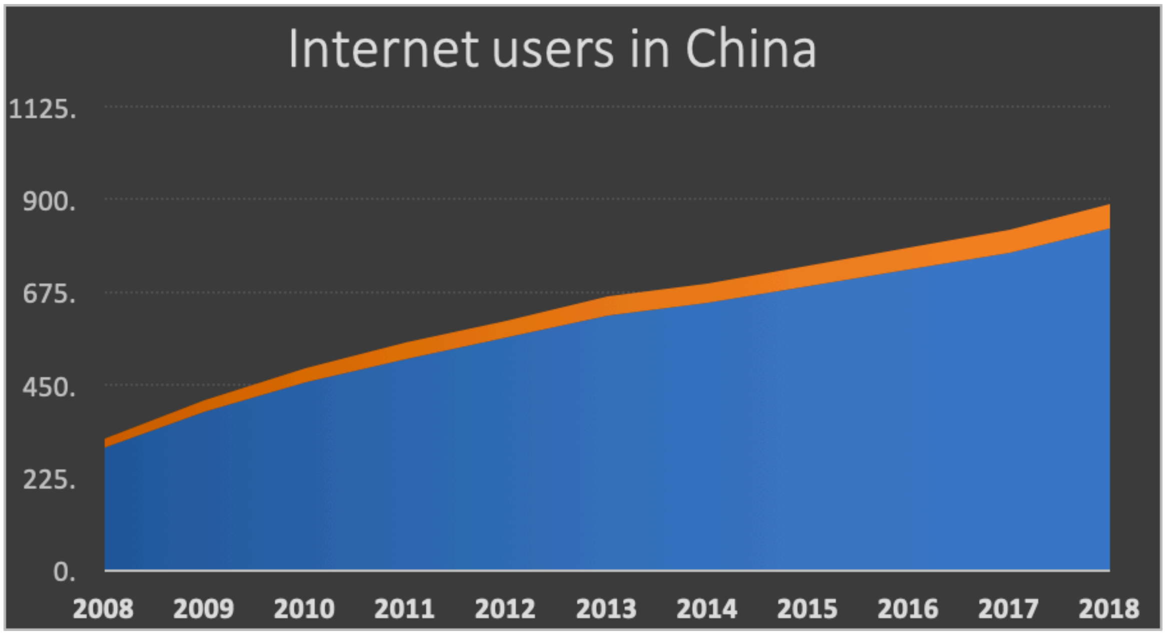
Secondly, given the stringent restrictions on internet content access, VPNs were the only source to access open information for people in China and circumvent the Great Firewall.[45] These were sources through which people could evade the censorship and access restricted websites with basic facilities such as emails and web search. The government, however, in an unprecedented policy move, instructed the telecommunication carriers to regulate access to VPNs.[46] The regulation on VPNs shut down the only window open for the people to access the contents beyond the regulated ones allowed by the government of China. This step by the CPC allowed it to have better control over the population by using regulations to reprimand people that build or use VPNs. The regulation was a consequence of the government's desire to ramp up cyber security and emphasis further on the concept of cyber sovereignty. At the same time, it was also a result of the government's growing repugnance towards the western liberal values which dominated the cyber domain.[47] This has been having unfavourable implications, especially on the people, without any marked detrimental intent towards the government or the country. Hence, this move has been criticized and saw protests, especially in the fields of art, music, and academia.[48]

However, the masses in China have used technological as well as linguistic creativity to circumvent the Firewall in China. While the VPNs were shut down by the government of China, there are still several VPNs such as Astrill, ExpressVPN, Hotspot Shield, ibVPN, Ivacy and more which enable masses to access blocked and censored websites and contents.[49] However risky it might be due to the fear of a backlash by the government, a sense of dissent towards the Party’s propaganda rules through technological inventions suggest some form of liberalism within the people living in China, at the same time a commitment towards science and technology, and a vigour to excel, embedded by Deng Xiaoping.

Further, censorship by the government demonstrates that China expects its citizens to be as apolitical as possible for the sustenance of its party’s ideology and governance. For the same, the CPC would clamp down any content and surveil any searches which it deems political and thus detrimental. In response to this, the people of China have devised a unique method of circumventing censorship by replacing taboo words with apolitical terms and phrases.

This can be characterised by the usage of terms such as *Check the Water Meter* which works as a euphemism for a house visit by the police; *Use the internet scientifically,* a phrase describing ways to circumvent Chinese censorship; *Great Chinese Lan,* a phrase describing the Chinese internet which unlike the internet infrastructure in the rest of the world is characterized by heavy censorship and the *River Crab* which similarly denotes the Chinese government censorship.[50] In fact, a book titled *China at the Tipping Point? From ‘Fart People’ to Citizens* was published by Perry Link and Xiao Qiang in 2013 which listed out slangs used by the masses to evade censorship.[51] This book was, later on, revised every year with new slangs till the year 2015, titled *Decoding the Chinese Internet: A Glossary of Political Slang*. This reiterated the creative techniques used by the people to exercise their opinion and put forward their views in front of the world through the medium of the internet.

Figure 1: Internet users in China



Source: Statista

The above figure demonstrates the increasing internet usage by people and the subsequent growth in internet traffic in China. It is in this regard that it can be argued that irrespective of the censorship and the crackdown of initiatives by people trying to circumvent the Great Firewall, people in China have increased their internet usage. To some extent, censorship evasion by people is working at a great level, and censorship is becoming counter-productive. However, it can also be argued that the government is successfully generating attractive alternatives to western technology by innovating its own technology which is, in turn, competing with the western counterparts.

It is in this context that, amidst the great amounts of censorship and cyber restrictions banning plethora of foreign websites such as Google, Facebook, Twitter, Instagram and more; China's domestic ecosystem has enabled the rise of Baidu, WeChat, TikTok and more which in fact in the view of current developments, successfully competing with its Western counterparts, irrespective of the censorship.[52] As a result, while China has stuck to its authoritarian form of governance, it hasn't compromised on its goals of economic and technological innovation and modernisation. The *fifty-cent army*, as discussed before, also remains a part of this. The above demonstrates the importance of the internet to be as significant to the Chinese government as it is for the Chinese people to diffuse their opinion. The above further reiterates how China considers the internet space as its strength to enhance the party legitimacy rather than a limit to CPC's governance.

Offensive Strategy to Offset Cyber Attacks

Recognizing the growing threats through cyberspace and its geopolitical and geo-economical competitions being more prevalent, China has been preparing for a cyberwar. The PLA is increasingly pursuing an ambitious cyber warfare agenda (the fifth dimension of warfare) that purports to link all the internet services through a common internet, communication and technology (ICT) platform which would have the capabilities to command at levels of informatisation, strategic planning and training services. [53] The Cyberspace is further being explored to be used for strengthening PLA activities.[54] Such a link between cyber and military was established first in a document released by China's Academy of Military Science, titled "Chinese Intelligence in Cyber Age."[55] However, according to many allegations, China's preparations for a cyber war went beyond strengthening its system's resilience, indulging in cyber espionage. In 2006-07, countries such as Germany, New Zealand and the United Kingdom reported cyber-attacks of Chinese origins.[56] Similar allegations were reported by Canada and even the Dalai Lama whose computer systems were attacked by a threat called Ghost-Net.[57] Subsequently, systems of Google were also attacked by a virus called Aurora, which aimed to access other systems of US corporations. Further, in 2012, the National Security Agency of the United States after investigations accused China of cyber espionage and the stealing of intellectual property.[58] The study further attributed to China an attack the previous year on systems of the RSA which are of national importance and dealt with classified work for the Pentagon.[59] As per the investigation report, these attacks were spear-phishing attacks[60] aimed at benefitting the R&D in China, where the host wanted to understand the workings of a system under attack and comprehend the entry points to the system to carry forward the attack. Such cyber developments have been relatively common between the US and China now, pushing them to the verge of a cyberwar. The cyber tensions between the US and China are classic examples to understand the US-China relations of global competition on the one hand and the perilous workings of cyberspace on the other.

The US Factor in China's Cyber Governance

International debates regarding the cyber domain have, more often than not, approached the arena as anarchic and unruly, which cannot be controlled or judicially restrained. The power of anonymity has enabled people to express their knowledge, capabilities and views; at the same time, it has facilitated millions of cyber-attacks. However, even while acknowledging the importance of cyberspace for its development, China did not disregard the need for filtration of content for the same. Nonetheless, the reasons to control the internet space for China go beyond national security to theoretical aspects. China, as a country entering the cyberspace relatively late in 1994, looks at the arena through the lens of technological inequality and Neo-Realism.[61]

The general argument put forward is that the low restrictions and institutionalization of cyberspace benefited the developed nations which had advanced their technology at the onset of the cyber era. However, the countries entering late and relatively nascent to the cyberspace, witnessed an extremely competitive and unequal environment, for which they were not prepared. This proved disadvantageous for the developing and the underdeveloped nations, while the technologically advanced – mainly the west – monopolized the space in accordance to its benefits. This was highly detrimental to China and its developing economy.[62] At the same time, this was the beginning of cyber friction between China and the US. For China then, cyber sovereignty becomes a tool to its sustain development and protect its interests at the face of the US using the internet to expand its influence and power. It does not trust the multi-stakeholder model of internet governance as it favours the US and allows it to exploit its advantages in the field of ICT.[63]

On the other hand, the US' recent announcement of considering China a 'revisionist' country could be looked at from a cyber front and draws its origins back to Xi Jinping's iteration of reforming the global cyber structure.[64] The US has condemned China's nonchalant approach towards human rights and its failure to maneuver within the gambits of the cyber standards set by international institutions. From the perspective of the US, its report by the Economic and Security Review Commission in 2018 to the US Congress had compiled many cases where viruses with Chinese origins had tried to attack systems of critical infrastructures or devices carrying information related to state security in the US.[65] It is in this context that the US accused China of violating an agreement that was signed by the then president of the United States, Barack Obama and the president of China, Xi Jinping in 2015.[66] According to this document, both China and the US agreed to refrain from activities related to cyber espionage, provide timely and accurate information regarding malicious cyber activities and cooperate to prevent cybercrime through a joint high-level dialogue mechanism.[67] However, the current president of the United States, Donald Trump accused China of violating the agreement in 2018.[68] Further, a report released by the US government recorded that China committed cyber espionage worth USD 300 billion in 2014.[69] While the numbers did decline post the agreement in 2015, US reports still recorded considerable amounts of cyber espionage by China thereafter.[70]

Thus, in May 2019, Donald Trump banned US companies dealing with Huawei in his Executive Order on Securing the Information and Communications Technology Services Supply Chain.[71] According to the government, the company had been carrying out cyber espionage and stealing intellectual property from the US. Subsequently, accusations against Huawei for intellectual property theft were made by telecommunication companies such as Cisco, Motorola, and T-Mobile. A similar allegation was carried out by the US against China's introduction of 5G, the fifth-dimensional wireless network. Importantly, as Huawei remains is a state-supported technological service, the competition regarding 5G in the domestic markets of China as well as markets in the global arena considerably reduces, favouring the company. The CPC's considerable command over Chinese private companies with Huawei's CEO Ren Zhengfei being a party member have been factors which remain at the helm of the suspicion over Huawei and Chinese tech companies in general.[72] This, when viewed keeping in mind the functionality of China's National Intelligence Law, only make matters more complicated.

In brief, the US and many other countries have started to acknowledge the strategic underpinnings of doing business with Huawei, and thus many are disallowing the company to participate in their 5G trials.[73] This comes from a developing perception amongst several countries regarding Chinese companies such as Huawei being actors of an authoritarian state, carrying values of unilateralism, opaqueness and revisionist desires.[74] Thus, China's cyber governance has been condemned by the US, which tries to ensure relatively free, open, and democratic cyberspace without much state control. And even if the US government does intrude by engaging in some form of cyber-surveillance, it does not officially deny it. In fact, the United States Department of Defense's Cyber Strategy states:

> *The Department must take action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests. Our focus will be on the States that can pose strategic threats to U.S. prosperity and security, particularly China and Russia.*[75]

Further, the report also states:

> *We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict. We will strengthen the security and resilience of networks and systems that contribute to current and future U.S. military advantages. We will collaborate with our interagency, industry, and international partners to advance our mutual interests.*[76]

The above statements reiterate the US perception of cyber security which remains as much offensive as defensive. Its cyber strategy, emphasizing on "Persistent engagement" and "defend forward" becomes an initiative to secure itself from cyber-attacks, especially from the state-sponsored ones by China and Russia. The cyber approach by the US has been a manifested shift from a defensive to an offensive posture as was demonstrated during the cyber strike by the US Cyber Command which took place during the military stand-off between US and Iran in the Persian Gulf.[77] This kind of offensive cyber posture by the US is not new. This was indicated when the ex-CIA systems analyst Edward Snowden exposed the US surveillance programme known as Prism which enabled the NSA to tap into the servers of internet firms such as Facebook, Google, Microsoft, Yahoo and more to track online communication.[78] This reiterated a covert, aggressive cyber posture by the US, which under the administration of President Donald Trump has become more prevalent and explicit.

However, Chinese leaders and officials claim that China possesses no offensive cyber capabilities and do not engage in cyber actions against states.Their contradictory cyber activities against several companies and countries only question the credibility of statements made by the CPC.[79] China has instead accused the US of carrying out its political agenda by placing allegations against China. It stated:

> *For a long time, relevant US government departments have instigated large-scale, organized online hacking activities against foreign governments, companies, and individuals.*[80]

Further, China has also criticised the US for exercising prejudiced and a threatening level of influence over the global cyber domain through the Internet Corporation for Assigned Names and Numbers (ICANN).[81] A distortion of facts from the Chinese side can be emphasized as the US cannot control the internet, even if the ICANN governance system originates from the US.[82] This statement, while indicating China's defensive approach towards tech politics with the US, also demonstrates its assertive and autarkic approach in preserving its technological advancement and economic growth. Another factor towards China's defensive approach has been the importance of 'prestige' and 'dignity' in Chinese culture denoted by the terms *Lian* and *mianzi.* The former term focuses on a "sense of shame in relation to social standards of morality and behaviour". The latter, *mianzi*, concentrates on saving face, prestige and social position. This demonstrates the importance of prestige and dignity in the Chinese culture, where the 'face' is considered far more psychological than physiological. In other words, the public image remains utmost important for China. It would portray itself as a nation which believes in the concept of "peaceful rise" and seek harmony. However, this equally remains contradictory to China's supposed posture in the cyber world. Another explanation for this remains what Sun Zu described as *subduing the enemy without fighting* as an essential art of war.[83] In this regard, the CPC in 2003 introduced the 'Three Warfares' as a strategy to win the war without going for a war, and at the same time-saving China's 'face.' These three strategies were:

Psychological Warfare–Undermines an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralizing the enemy military personnel and supporting civilian populations.

Public Opinion/Media Warfare–Influences domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests.

Legal Warfare–Uses international and domestic law to claim the legal high ground or assert Chinese interests.[84]

Thus, China uses these strategies to mould a tensed situation according to its interest in such a way that its activities or reactions are not questionable in the domestic or international domain. China, through its cyber sovereignty, is altering the course of cyber content according to its own will in its domestic domain to ensure the legitimacy of the CPC. At the same time, China focuses on acquiring information as a foundation for its cybersecurity and as a defensive strategy.[85]

China's Cyber Governance and the Covid-19 Pandemic

Even though the CPC under the guidance of Xi Jinping has been successful in controlling the information flow through its policies guided by its concept of cyber sovereignty, it has not been devoid of criticisms at home. One of the major instances of this has taken place amidst the Covid-19, as the pandemic has proven to be one of the biggest challenges to Xi's leadership and authority since he assumed power in 2012. The consolidation of power and his capability to ensure stability and control are being questioned and condemned as China was unable to suppress the Novel Coronavirus from spreading outside its territory. Moreover, the outbreak highlighted the lack of transparency and openness of the Chinese authorities, with early warnings by scientists and medical professionals being dismissed or suppressed. In particular, the censoring of critical information regarding the spread of the virus in China during the early stages of the pandemic in China, along with the suppression of voices being critical towards the government's conduct during the pandemic had been condemned by Chinese citizens, as well as international spectators.[86] In fact, the interrogation of Dr Li Wenliang by the authorities for posting information about the Novel Coronavirus in the online platform of WeChat groups, and his subsequent death reignited outrage over the CPC's suppression of dissent.[87] The enhancement of surveillance by the government on social media platforms following with suppression of voices, and along with a greater emphasis on the fifty-cent army to overshadow the criticisms with the CPC's propaganda also received disparagements. If anything, China's aggressive suppression of dissent on the internet resonated its overestimating capacity to control the crisis led by persistent resistance from the Chinese citizens, as well as censures from the international community.

Further criticisms were prevalent as China unveiled its new powers to censor Hong Kong's internet access using its recent introduction of the National Security Law in the region. China has received a considerable amount of resistance from the people of Hong Kong and a significant amount of protests from the international community, and particularly by the US tech giants.[88] The point of concern which has the potential to threaten Hong Kong's unique freedoms as per the joint declaration between China and Britain during Hong Kong's handover remains the city's Chief Executive- a pro-Beijing appointee- having the powers to approve applications for interception and covert surveillance operations, threatening the national security of Hong Kong, as well as the international community connected to the region; thus, having global consequences.[89]Even as China's control over the internet and its surveillance network seem formidable, these developments do stand as potential corrosion to the authority of Xi Jinping. These, if anything, signify towards the growing and widespread public demand for government accountability in China, which is putting pressure on the regime and the leader. This, arguably, would only enhance post the Covid-19 episode, creating greater challenges for CPC and Xi Jinping.

Conclusion

This paper, from the means of evaluating China's approach to cyberspace, examined its adoption of the internet and its transformation to a restricted and regulated framework. It argued that while adopting such a framework, China did not compromise on its competences in the field of technology and innovation; instead, it has only strengthened its techno-capabilities. Through the same argument, the paper has linked China's domestic scenario with the frictions it is witnessing in the international forum. Certainly, China's intent to regulate the information flow in China and control the cyberspace inside its territory would remain prevalent. However, China's security perceptions, as well as its policies regarding the cyber domain might have to cater to a modified post COVID-19 environment, where its ability to influence the domestic affairs through restrictions and regulations might face resistance and greater challenges. Further, the international community is gradually becoming active in criticizing China's cyber policies and activities, which, to a certain extent, has been affecting the security of other countries.

Endnotes

[1] Zhao Lei and Cao Yin, 'President Xi vows to boost cybersecurity', *China Daily*, February 28, 2014, http://www.chinadaily.com.cn/china/2014-02/28/content_17311483.htm (accessed September 6, 2019).

[2] 'Full Text of Jiang Zemin's Report at 16th Party Congress', China.org.cn, http://www.china.org.cn/english/features/49007.htm (accessed September 6, 2019).

[3] Nigel Inkster, 'China and Cyber Sovereignty,' *Asia Dialogue,* September 4, 2018, https://theasiadialogue.com/2018/09/04/china-and-cyber-sovereignty/ (accessed September 6, 2019).

[4] 'Full text of Hu Jintao's report at 18th Party Congress', Embassy of the People's Republic of China in the United States of China, November 27, 2012, http://www.china-embassy.org/eng/zt/18th_CPC_National_Congress_Eng/t992917.htm (accessed September 6, 2019).

[5] Jason Fritz, 'How China will use Cyber Warfare to Leapfrog in Military Competitiveness', *Culture Mandala: The Bulletin for the Centre for East-West Cultural and Economic Studies*, 8(1), October 1, 2008, https://pdfs.semanticscholar.org/d8ce/036ab6a23051b2244a34f5cf70455270f421.pdf (accessed September 6, 2019).

[6] Hu Jintao, 'Hu urges innovation in science, technology', Government of China, January 9, 2006, http://www.gov.cn/english/2006-01/09/content_151631.htm (accessed September 6, 2019).

[7] China's GDP per capita as of 2019 was $10,276, which though growing at a considerable rate, is still less in comparison to a few other developed nations. Hence, as stated in the 19th Party Congress, China aims to become a high-income nation (per capita) by 2030. Please see, 'China's GDP per capita just passed $10,000, but what does this mean?', *CGTN*, January 17, 2020, https://news.cgtn.com/news/2020-01-17/China-s-GDP-per-capita-just-passed-10-000-but-what-does-this-mean--NkvMWAMYNO/index.html#:~:text=China's%20GDP%20per%20capita%20reached,moderately%20prosperous%20society%22%20in%202020. (Accessed on August 20, 2020)

[8] Xi Jinping, 'Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for New Era,' *Work Report delivered at the 19th National Congress of the Communist Party of China*, October 18, 2017, https://mp.weixin.qq.com/s/EpdgYurAxZ2bnKZnZuenfg (accessed September 6, 2019).

[9] Chan Jia Hao, 'China's Digital Silk Road: A Game Changer for Asian Economies', *The Diplomat*, April 30, 2019, https://thediplomat.com/2019/04/chinas-digital-silk-road-a-game-changer-for-asian-economies/. (Accessed on August 23, 2020)

[10] The 'Chinese Dream of national rejuvenation' propounded by Xi Jinping refers to the dream of the great renewal of the Chinese nation through achieving prosperity, power and happiness for all its people. Please see, "Background: Connotations of Chinese Dream", China Daily, March 05, 2014, https://www.chinadaily.com.cn/china/2014npcandcppcc/2014-03/05/content_17324203.htm; John Garrick and Yan Chang Bennett, "Xi Jinping Thought: Realisation of the Chinese Dream of National Rejuvenation?", *China Perspectives*, No. 2018/1-2, 2018, pp. 96-106.

[11] Robert Greene and Paul Triolo, 'Will China Control the Global Internet Via its Digital Silk Road', *Carnegie Endowment for International Peace*, May 08, 2020, https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857. ((Accessed on August 23, 2020)

[12] Please read, Cai Cuihong, "Cybersecurity in the Chinese Context: Changing Concepts, Vital Interests, and Prospects for Cooperation", *China Quarterly of International Strategic Studies*, Volume I, No. 3, 2015, 471-496.

[13] Please read, RogierCreemers. 2017. 'Cyber-Leninism: The Political Culture of the Chinese Internet' in Monroe Price and Nicole Stremlau (Eds.), *Speech and Society in Turbulent Times: Freedom of Expression in Comparative Perspective*. Cambridge: Cambridge University Press, 255-273;Jinghan Zeng, Tim Stevens and Yaru Chen, 'China's Solution to Cyber Governance: Unpacking the Domestic Discourse of Internet Sovereignty', *Politics and Policy*, Volume XLV, No. 3, 2017, 432-464.

[14] Han, Rongbin. 2018. *Contesting Cyberspace in China,* New York: Columbia University Press, 250-256

[15] The Great Firewall physically controls the internet architecture and censors the flow of online information. This internet infrastructure of China uses multiple censorship techniques such as automatically filtering taboo words to manually surveile the internet. Other techniques involve limiting access to undesired websites, shutting them down and even detaining the dissenters. Please see Han, Rongbin. 2018. *Contesting Cyberspace in China,* New York: Columbia University Press, 87-90; James Griffiths. 2019. 'Nailing. The Jello: Chinese Democracy and the Great Firewall', *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet.* London: Zed Publications, 77-90.

[16] Elizabeth C. Economy, 'The great firewall of China: Xi Jinping's internet shutdown', *The Guardian*, June 29, 2018, https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown. (Accessed on November 3, 2019)

[17]For more arguments, please read, Rongbin Han, "Manufacturing Consent in Cyberspace: China's "Fifty-Cent Army", *Journal of Current Chinese Affairs*, Volume XLII, No. 2, 105-135
[18]Please see, Li Jing, 'Revealed: the digital army making hundreds of millions of social media posts singing praises of the Communist Party, *South China Morning Post*, May 19, 2016, https://www.scmp.com/news/china/policies-politics/article/1947376/revealed-digital-army-making-hundreds-millions-social. (Accessed on August 23, 2020)

[19]According to a report by Statista titled "Most valuable technology brands worldwide in 2020", Chinese companies such as Tencent, Huawei, Baidu, and Xiaomi held the top positions globally. In fact, held the fourth most valuable technology brand position with $150.98 billion brand value, succeeding by Huawei at the 15th position, Xiaomi at the 19th position and Baidu at the 20th position with $29.4 billion, $16.6 billion and $14.84 billion brand value, respectively. At present, Huawei remains the 5G face of China, having the capability to provide 5G technology ensuring seamless AI functions seamlessly. While the 5G technology is turning into a battleground between the US and China, Huawei might have proven to be the Trojan horse. Thomas Alsop, 'Most valuable technology brands worldwide in 2020', *Statista*, July 15, 2020, https://www.statista.com/statistics/267966/brand-values-of-the-most-valuable-technology-brands-in-the-world/. (Accessed on August 24, 2020); Keith Johnson and Elias Groll, 'The Improbable Rise of Huawei', April 03, 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/. (Accessed on August 24, 2020)

[20] Niall McCarthy, 'China now boasts more than 800 million internet users and 98% of them are mobile', *Forbes,* August 23, 2018, https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/#2cb196187092 (accessed September 7, 2019).

[21]See 'President Xi Jinping's speech in the first session of the Central Leading Group for Cyberspace Affairs', *Cyberspace Administration of China website*, February 27, 2014, http:// www.cac.gov.cn/2014-02/27/c 133148354.htm. (Accessed on August 23, 2020)

[22] The CNP could be defined as the combined weight of economic, diplomatic and military power. From a state-centric perspective, such power would be necessary for China to fulfil its

aim of guaranteeing ‘appropriate influence at the world stage’. These are not military goals *per se*, but institutional goals tied to China’s national objectives.

[23]Please note, the core strategic interests mentioned in this paper are inferences made by the author based on the arguments made in the sources below. Please see, Kevin Rudd, ‘The Coronavirus and Xi Jinping’s Worldview’, *Project Syndicate*, February 8, 2020, https://www.project-syndicate.org/commentary/coronavirus-will-not-change-xi-jinping-china-governance-by-kevin-rudd-2020-02 (accessed April 7, 2020); ‘China's Foreign Policy in a Fast Changing World: Mission and Responsibility – Speech by Vice Foreign Minister Le Yucheng at the Lunch Meeting of the Eighth World Peace Forum’, Ministry of Foreign Affairs of the People’s Republic of China, July 8, 2019, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1679454.shtml (accessed April 7, 2020); ‘Full Text: China's National Defense in the New Era’, *Xinhua*, July 24, 2019, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm (accessed April 7, 2020).

[24] Zhao Lei, ‘Xi vows to fight ‘three evil forces’ of terrorism, separatism, and extremism’, *China Watch,* June 19, 2017, https://www.telegraph.co.uk/china-watch/politics/xi-fights-three-evil-forces-terrorism-separatism-extremism/ (accessed September 7, 2019).

[25] ‘Cyber Security: An Overview’, *IDSA Task Force Report,* 2012, 24–25; Please read, David Bernard-Wills, Debi Ashenden, ‘Securing Virtual Space: Cyber War, Cyber Terror, and Risk, *Space and Culture*, Volume XV, No. 2, March 21, 2012, 110–123

[26] Aeron D. McGeary, ‘China's Great Balancing Act: Maximizing the Internet's Benefits While Limiting Its Detriments’, *The International Lawyer*, Volume XXXV, No. 1, 2001, 223–224.

[27] Ibid.

[28] ‘The Constitution of the People’s Republic of China’, *The National People’sCongress of the People’sRepublic of China*, March 14, 2004, https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn147en.pdf (accessed September 6, 2019).

[29] ‘The Internet in China,’ *Information Office of the State Council of the People's Republic of China*, June 8, 2010, http://www.gov.cn/english/2010-06/08/content_1622956_3.htm (accessed September 6, 2019).

[30] Ibid.

[31] ‘2013 China Diplomatic White Paper: China’s determination to maintain territorial sovereignty is firm (reproduced)’, *People’s Daily Online*, July 17, 2013, http://bbs.tianya.cn/post-worldlook-827386-1.shtml (accessed September 6, 2019).

[32] Please read, SevereneArsrene, ‘Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic Order?’ *China Perspectives*, Volume 2, No. 106, 2016, 25-35

[33] Ibid.

[34] 'International Strategy of Cooperation on Cyber Space', *Xinhua*, March 1, 2017, http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm. (Accessed on September 6, 2019)

[35]'National Intelligence Law of the People's Republic of China_中国人大网', *The National People's Congress of the People's Republic of China*, June 27, 2017, https://cs.brown.edu/courses/csci1800/ sources/2017_PRC_NationalIntelligenceLaw.pdf. (Accessed on August 23, 2020); Bonnie Girard, 'The Real Danger of China's National Intelligence Law', *The Diplomat*, February 23, 2019, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/. (Accessed on August 23, 2020)

[36]Lauren Maranto, 'Who Benefits from China's Cybersecurity Laws?', *Center for strategic and International Studies (CSIS)*, June 25, 2020, https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws#:~:text=In%20June%202017%2C%20the%20China,for%20China's%20present%20day%20guidelines.&text=The%20law%20requires%20that%20data,to%20government%2Dconducted%20security%20checks. (Accessed on August 23, 2020)

[37] Elsa B. Kania, 'China's Strategic Support Force At 3', *TheDiplomat*, December 29, 2018, https://thediplomat.com/2018/12/chinas-strategic-support-force-at-3 (accessed September 7, 2019).

[38] Ibid.

[39] Jiang Jie, 'China unveils its first civil-military cybersecurity innovation center', *People's Daily*, December 28, 2017, http://en.people.cn/n3/2017/1228/c90000-9309428.html (accessed September 7, 2019).

[40] Ibid.

[41]Eunju Chi, 'Chinese Government's Responses to Use of the Internet', *Asia Perspectives,* Volume XXXVI, No. 3, July-September 2012, 387-409.

[42] 'Is Internet Access a Human Right?' *Amnesty International,* https://www.amnestyusa.org/is-internet-access-a-human-right/ (accessed September 7, 2019).

[43] Nina Hachigian, "China's Cyber Strategy", *Council on Foreign Relations,* Volume LXXX, No. 2, March April 2002, 123–128.

[44] Ibid.

[45] Virtual Private Network (VPN) are networks that are capable of circumventing the restrictions and censorships by the government on internet content. For more information, please see Michael Tann and Lynn Zhao, Use of VPNs facing challenges in China, *Global Data Hub,* July 2017, https://globaldatahub.taylorwessing.com/article/use-of-vpns-facing-new-challenges-in-china (accessed September 7, 2019)

[46] Samson Yuen, 'Becoming a Cyber Power: China's Cybersecurity Upgrade and its Consequences', *China Perspectives*, Volume MMXV, No. 2, June 1, 2015, 53-54

[47] Ibid.

[48] Ibid.

[49] P.H Madore, '13 VPNs Guaranteed to Help You Escape China's Ironclad Great Firewall', *CCN,* May 28, 2019, https://www.ccn.com/13-vpns-escape-china-great-firewall/. (Accessed on November 3, 2019)

[50]KuangKengKuek Ser, 'Want to circumvent China's Great Firewall? Learn these 9 phrases first', *pri.org*, July 20, 2015, https://www.pri.org/stories/2015-07-20/want-circumvent-chinas-great-firewall-learn-these-9-phrases-first. (Accessed on November 3, 2019); Anna Fifield, 'These are the secret code words that let you criticize the Chinese government', *The Washington Post,* August 4, 2015, https://www.washingtonpost.com/news/worldviews/wp/2015/07/29/these-are-the-secret-code-words-that-let-you-criticize-the-chinese-government/. (Accessed on November 3, 2019)

[51] 'Decoding the Chinese Internet: A Glossary of Political Slag', *China Digital Times,* June 2015, https://monoskop.org/images/b/b7/Decoding_the_Chinese_Internet_A_Glossary_of_Political_Slang_2015.pdf. (Accessed on November 3, 2019)

[52] Please refer to footnote no. 18.

[53] Nigel Inkster, "Chinese Intelligence in Cyber Age", *Survival,* Volume LV, No. 1, January 31, 2013, 23; Also see, 'The Science of Military Strategy', *The Academy of Military Science,* https://fas.org/nuke/guide/china/sms-2013.pdf (accessed September 7, 2019).

[54] Larry M. Wortzel, 'China's Military Modernization and Cyber Activities: Testimony of Dr. Larry M. Wortzel before the House Armed Services Committee', *Strategic Studies Quarterly,* Volume VIII, No. 22, 2014, 3–22.

[55] The Academy of Military Science, no. 53.

[56] Nigel Inkster, no. 53.

[57] Ibid.

[58] Colin Clarke, 'China Attacked Internet Security Company RSA, General Tells SASC', *AOL Defense*, March 27, 2012.

[59] Ibid.

[60] Spear-phishing attacks are attacks towards an individual or a group which is carried out by sending emails to targeted systems. Once attacked, the virus such as Trojan is capable of providing remote access to the targeted network. For more information, please see, 'The Impact of Usability on Phishing: prevention effectiveness', *Cyber Defense Magazine*, April 13, 2019, https://www.cyberdefensemagazine.com/the-impact-of-usability-on-phishing-prevention-effectiveness/ (accessed September 7, 2019).

[61]Within the Neo-Realist discipline of thought, rational states in an anarchical environment, seek to enhance their security by maximizing their capabilities and power to ensure survival. They do so due to the lack of trust factor, especially towards the US, which leads them operate in a self-help system. China, with its domestic conditions and international position prevalently holds this approach towards the cyber domain to ensure the sustenance of its regime, its ideology and enhance its national development. Please read, Francis C. Domingo, 'Conquering a new domain: Explaining great power competition in cyberspace', Comparative Strategy, Volume XXXV, No. 2, 2016, 154-168.

[62] Ibid.

[63] Yi Shen, 'Cyber Sovereignty and the Governance of Global Cyberspace', *Chinese Political Science Review*, Volume I, No. 1, March 2016, 91.

[64] 'National Defense Strategy of United States of America, 2018', *Government of the United States*, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. (accessed September 6, 2019).

[65] 'Report to Congress of the US-China Economic and Security Review Commission, 2018', *USCC 2018 Annual Report*, November 2, 2018, 19, at https://www.uscc.gov/sites/default/files/annual_reports/2018%20Annual%20Report%20to%20Congress.pdf (accessed September 7, 2019).

[66] John W. Rollins, 'US-China Cyber Agreement', *CRS Insight*, October 16, 2015, https://fas.org/sgp/crs/row/IN10376.pdf (accessed September 7, 2019).

[67] Ibid.

[68] 'U.S. accuses China of violating bilateral anti-hacking deal', *Reuters*, November 9, 2018, https://www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E (accessed September 7, 2019).

[69] 'Chinese cyber-attacks on targets in US have plummeted, say experts', *South China Morning Post,* June 21, 2016, https://www.scmp.com/news/china/diplomacy-defence/article/1978361/chinese-cyber-attacks-targets-us-have-plummeted-say (accessed September 7, 2019).

[70] 'Cyber Espionage and the Theft of U.S. Intellectual Property and Technology', *Government of the United States*, 2014, at https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm (accessed September 7, 2019).

[71] 'Executive Order on Securing the Information and Communications Technology Services Supply Chain', *White House*, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ (accessed September 7, 2019).

[72]Marc Santora, 'Pompeo Calls China's Ruling Party Central Threat of Our Times', *The New York Times*, January 30, 2020, at https://www.nytimes.com/2020/01/30/world/europe/pompeo-uk-china-huawei.html?auth=redirect-apple. (Accessed on August 22, 2020)

[73]Countries which have banned the products and services of Huawei either implicitly or explicitly include Australia, New Zealand, Vietnam, Taiwan, Japan, Poland, Czech Republic, Denmark, Estonia, Latvia, Romania, the UK, and the US. There are several countries which are still weighing their options regarding Huawei. Please see, Michael R. Pompeo, 'Welcoming the United Kingdom Decision to Prohibit Huawei from 5G networks', *US Embassy in Mauritania*, July 14, 2020, https://mr.usembassy.gov/welcoming-the-united-kingdom-decision-to-prohibit-huawei-from-5g-networks/. (Accessed on August 20, 2020); Joe Panettieri, 'Huawei: Banned and Permitted in Which Countries? List and FAQ', *Channele2e*, August 20, 2020, https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/. (Accessed on August 20, 2020)

[74]Jagannath P. Panda, 'India must stay alert to Beijing's techno-national gambit', *The Sunday Guardian*, May 23, 2020, https://www.sundayguardianlive.com/news/india-must-stay-alert-beijings-techno-national-gambit. (Accessed on August 21, 2020)

[75] 'Cyber Strategy 2018', *Department of Defense, Government of United States,* September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. (Accessed on November 3, 2019)

[76] Ibid.

[77] Nicole Lindsey, 'US Cyber Command Signals More Aggressive Approach Involving Persistent Engagement Ahead of 2020 Election', *CPO Magazine,* September 16, 2019, https://www.cpomagazine.com/cyber-security/us-cyber-command-signals-more-aggressive-approach-involving-persistent-engagement-ahead-of-2020-election/. (Accessed on November 3, 2019)

[78] 'Edward Snowden: Leaks that Exposed US Spy Programme', *BBC News,* January 17, 2014, https://www.bbc.com/news/world-us-canada-23123964. (Accessed on November 3, 2019)

[79] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations", *China Leadership*, September 20, 2013, No. 42, 15.

[80] Edward White, Alice Woodhouse, and Xinning Liu, ‘China hits back at US and UK allegations of cyber-attacks’, *Financial Times,* December 21, 2018, https://www.ft.com/content/47eb9b12-04da-11e9-99df-6183d3002ee1 (accessed September 7, 2019).

81Cao Siqi, ‘Intl cooperation enhances China’s role in net connectivity, safeguarding cyber sovereignty’. *Global Times*, January 13, 2020, https://www.globaltimes.cn/content/1176677.shtml (Accessed on August 20, 2020).

[82] ICANN was created in 1998 to perform technical coordination of the internet. Its functions include the laying of foundations for governance and creating capabilities to enforce global regulations on the internet use. Please read Hans Klein, ‘ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy’, *The Information Society*, Volume XVIII, No. 3, 2002, 193-207.

[83] Sun Tzu. 2010. *The Art of War*. Translated by Lionel Giles. Pax Librorum Publishing House, 2008.

[84] ‘Military and Security Developments Involving the People’s Republic of China 2011’, *Office of the Secretary of Defense Annual Report to Congress*, 2011, http://www.defense.gov/pubs/pdfs/2011_CMPR_Final.pdf. (accessed September 7, 2019).

[85]LyuJinghua, ‘What are China’s Cyber Capabilities and Intentions?’, *Carnegie Endowment for International Peace,* April 1, 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734 (accessed September 7, 2019).

[86]Jane Li, ‘Martian language, emoji, and braille: How China is rallying to save a coronavirus story online’, *Quartz*, March 11, 2020, https://qz.com/1816219/chinese-internet-rallied-to-save-a-censored-coronavirus-story/. (Accessed on August 20, 2020)

[87]Kuang Biao, ‘China’s coronavirus cover-up: how censorship and propaganda obstructed the truth’, *The Conversation*, March 07, 2020, https://theconversation.com/chinas-coronavirus-cover-up-how-censorship-and-propaganda-obstructed-the-truth-133095. (Accessed on August 20, 2020)

[88]Ahence France-Presse, ‘China censors internet in Hong Kong’, *The Hindu*, July 07, 2020, https://www.thehindu.com/news/international/china-censors-internet-in-hong-kong/article32015853.ece. (Accessed on August 20, 2020)

89Steven Feldstein, ‘China’s Latest Crackdown in Hong Kong Will Have Global Consequences’, *Carnegie Endowment for International Peace,* July 09, 2020, https://carnegieendowment.org/2020/07/09/china-s-latest-crackdown-in-hong-kong-will-have-global-consequences-pub-82264. (Accessed on August 20, 2020)

ICS OCCASIONAL PAPER *Back Issues*

ICS Occasional Papers showcase ongoing research of ICS faculty and associates on aspects of Chinese and East Asian politics, international relations, economy, society, history and culture.

Issue No/ Month	Title	Author
No.54| Aug 2020	Traditional Cultural Ideas and Symbols, and Possibilities of Discursive Legitimacy in Contemporary China	Devendra Kumar
No.53| Jul 2020	What Future for India-China Economic Relations?	Ravi Bhoothalingam
No.52| Jul 2020	Student Mobility for Higher Education: The Case of Indian Students Studying Medicine in China	Madhurima Nundy and Rama Baru
No. 51| Jun 2020	Analyzing China's Mediator Role in MENA - More than Just a Global Responsibility?	Jayshree Borah
No.50| May 2020	Launch-On-Warning and China's Nuclear Posture	Samanvya Hooda

PRINCIPAL SUPPORTERS TO ICS RESEARCH FUND

TATA TRUSTS

MINISTRY OF EXTERNAL AFFAIRS
GOVERNMENT OF INDIA

INDIAN COUNCIL OF
SOCIAL SCIENCE RESEARCH

GARGI AND VIDYA
PRAKASH DUTT FOUNDATION

JAMNALAL BAJAJ
FOUNDATION

PIROJSHA GODREJ FOUNDATION

ICS PUBLICATIONS

ICS ANALYSIS
A short brief on a topic of contemporary interest with policy-related inputs

ICS OCCASIONAL PAPER
Platform for ongoing research of the ICS faculty and associates

ICS MONOGRAPH
Authored by the faculty, also emerging from research projects and international conferences

ICS WORKING PAPER
Draft paper of ongoing research

ICS JOURNAL

In its 56th year, *China Report* is a refereed journal in the field of social sciences and international relations. It welcomes and offers a platform for original research from a multi-disciplinary perspective, in new and emerging areas, by scholars and research students. It seeks to promote analysis and vigorous debate on all aspects of Sino-Indian relations, India-China comparative studies and multilateral and bilateral initiatives and collaborations across Asia.

China Report is brought out by Sage Publications Ltd, New Delhi.

Editor	Sreemati Chakrabarti
Associate Editor	G. Balatchandirane
Assistant Editor	Rityusha Mani Tiwari
Book Review Editor	Vijay K Nambiar

INSTITUTE OF CHINESE STUDIES
8/17, Sri Ram Road, Civil Lines,
Delhi 110054, INDIA
T: +91 (0) 11 2393 8202
F: +91 (0) 11 2383 0728

http://www.icsin.org/
info@icsin.org

twitter.com/ics_delhi
In.linkedin.com/Icsdelhi
youtube.com/ICSWEB
facebook.com/icsin.delhi
soundcloud.com.ICSIN
instagram.com/icsdelhi