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. She is also an editorial assistant to the Series Editor for *Routledge Studies on Think Asia*. She has previously worked for the East Asia Centre, at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) as a Project Assistant. She primarily focuses on China's foreign policy and strategic affairs. Her themes of research also include the geostrategic affairs of the Indo-Pacific region and East Asia's geopolitics and security studies. Her recent works include, "China and Quad 2.0: Between Response and Regional Construct" in *Maritime Affairs*, the Journal of National Maritime Foundation of India (NMF) and "Xi Jinping's India Policy" in *Eurasia Review*. She has also written for the Institute for Security and Development Policy (ISDP), Sweden, the *Journal for Indian and Asian Studies (JIAS)*, *World Focus*, *World in One News (WION)*, *Business Today*, *Defense and Security Alert (DSA)* and *The Pioneer*.

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 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 China's cybersecurity law. China has been propagating the concept of 'cyber sovereignty,' extending its influence to the fifth dimension and providing a competitive alternative to the multi-stakeholder model 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 cyber governance targets an overhaul of the internet, aiming to secure its cyberspace, reducing dependence on foreign technology, acquiring the ability for surveillance and controlling online information inside its territory. While its technological developments are resulting in economic growth, advances in surveillance, data mining, as well as artificial intelligence, have been having significant implications on the Chinese society. At the same time, while few countries have been in synergy with the Chinese approach of internet governance, several other countries, including the United States (US) have accused China of cyber espionage and targeting sensitive data in their territory. In this context, this paper aims to examine China's vision of cyber sovereignty through the underpinnings of national security, economic development, and societal interests. It further purports to assess the implications of China's cyber sovereignty in the domestic as well as in the global arena, particularly in the backdrop of a growing US-China cyber conflict. Lastly, it aims to highlight the challenges to China's cyber governance, having possible repercussions for the legitimacy of the leadership in the post-COVID-19 period.

Key Words: Cyber governance, 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 perception of cyber governance. Contrary to the multi-stakeholder vision[1] of an open and inclusive cyberspace, China has promulgated an authoritarian space where its governance factorises regulations and restrictions. This form of governance stems from China's conception of cyber sovereignty, which signifies that it will choose a development intensive path which 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 (adequate defensive and offensive cyber capabilities, in terms of key national infrastructure and requisite deterrence in regard to cyber and military security). Further, it would target to establish a globally competitive internet industry, 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 friction with countries such as the US, leading to debates and deliberations regarding the 'correct form' of cyber governance.

This paper, essentially, examines China's cyber governance and its vision in an increasingly contested international cyber domain. It argues that China's cyber governance model is a unique juxtaposition of an authoritarian government controlling the flow of information inside China through regulations and restrictions; and at the same time, emphasising on technological advancement and strengthened internet. Further, China's cyber governance model diverges from the multi-stakeholder model of internet governance, resulting in frictions with countries endorsing an open and inclusive cyber domain with uncontrolled information flow. Keeping the central argument of the paper in mind, the article analyses how China's domestic compulsions and national security considerations have increasingly shaped its cyber sovereignty. While doing so, the paper examines the implications of China’s cyber governance on its domestic as well as on its external environment.

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 for ‘China as a strong Cyber Power’ in his remarks during the first meeting of a central Internet security and informatisation leading group.[2] Further, Xi vowed to acquire national power by utilising the complete benefits of the internet.[3] However, in retrospect, 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 national economic progress.[4] These pushed China closer to modernisation, with science and technology as the pillars of socio-economic development. Subsequently, Jiang Zemin promulgated the development and utilisation of IT in all areas of China’s social and economic advancement.[5] He emphasised on the importance of IT and the utilisation of Information and Communication Technology (ICT) to bring about a leapfrog development in China’s modernisation.[6] However, the term ‘cyber’ was first mentioned by Hu Jintao in his report of the 17th Party Congress in 2007.[7] This was mainly after a series of Denial of Service (DoS) attacks on Estonia which targeted its parliament, government ministries, major banks, and media that lead Estonia to come to a complete standstill.[8] 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 emphasise on regulating 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 modernisation.[9] Thus, Hu Jintao, during the 18th Party Congress emphasised on the important maritime, space, and cybersecurity areas, which were to shape China’s policies and priorities, focussing on the cyberspace in the coming years.[10] 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.’[11] For Xi, a modernised economy with technological strength contributes to the country’s Comprehensive National Power

(CNP) [12] and its international stature. Hence, China has been increasingly integrating its economy with technology. One of the best examples of this has been the development of the Belt and Road Initiative (BRI) which has been expanded to include science and technology. [13] Under the banner of the BRI, China seeks to establish the Digital Silk Road (DSR), which aims to focus on building a digital and smart connectivity infrastructure; deepen space cooperation; develop common technology standards; and improve the efficiency of regulating systems amongst the BRI countries.[14] 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.[15] However, in the backdrop of China's authoritarian management of the cyber domain and its goal to attain the "Chinese Dream" of national rejuvenation[16], the DSR can be argued as a vehicle for China's control over the global cyberspace and a masterplan to deploy its regulatory model along with the BRI countries. [17] This argument could be better proven by comprehending China's cyber management under Xi Jinping.

Xi, during the 19th CPC National 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 the party work has been developing and strengthening the CPC's functionality. 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, leading to the augmentation of the party legitimacy. Further, Xi Jinping's speech during the 19th CPC National Congress 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.*[18]

This statement expressed the core principles of China's vision of cyber governance. It reiterated the 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.[19] This step is supported by the law of the government of China and would account for stern 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), which was established in 2014 and is currently led by Xi Jinping. Other stakeholders include the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS). Notably, 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 (SCIO), respectively. This essentially reverberates the significant role of the CPC's propaganda in China's cyber governance, allowing it to shape the views of the Chinese society.

Further, 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, while 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.[20] Importantly, there is a significant amount of state control on online news publication as a medium of surveillance and control. Only state-run news agencies such as Xinhua News Agency, China Global Television Network (CGTN), China Central Television (CCTV), People's Daily, China News Service (CNS) and more, are able to produce news, while the rest are allowed to reprint; as a mode of occupation of the cyberspace by the state.

More importantly, China has devised the Great Firewall, a combination of legal actions and technology to regulate the internet through censorship.[21] 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 flowing through it to overload targeted websites, leading it to go down.[22] The above restate the core principles of cyber governance by the CPC, which emphasis controlling the cyber domain according to its ideologies and ensuring absolute power over China's territory and people. However, what is intriguing about cyber 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.

Akin to the Arab Spring, where social media networks played an important role in the rapid disintegration of regimes in Tunisia and Egypt while contributing to sociopolitical mobilisation in Syria and Bahrain,[23] advancement in online expression in China 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.[24] 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 utilising 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.[25] 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 through technological areas of Artificial Intelligence (AI), and telecommunication giants of Huawei, Alibaba, ZTE, Tencent, and more which are increasingly enhancing their global footprint,[26] China and its 854 million internet users[27] are not immune to cyber threats and cyber attacks. Its principles of cyber governance are as much built on a defensive strategy to secure 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 of land, sea, or air. It has become much more unconventional. The fear is that a cyber-attack (cyber terrorism, cyber espionage, cybercrimes) on China's critical infrastructures by a state or even a third party 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 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 informatisation, no modernisation. Only by using security to guarantee development and using development to promote security, can long-term peace and order be realised'.*[28]

Xi's speech denoted the significance for China to strengthen its grip over the internet to meet its national goals. One of the significant drivers for China's emphasis on internet control remains 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, 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 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 East China Sea and the South China Sea; Pushing back the influence of the US 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 universally accepted.[29]

Another major factor for China's authoritarian control over the internet remains its concept of the "Three Evils/Three Evil forces"- terrorism, extremism, and separatism.[30] China's defence white papers have, time and again, expressed commitment in combating the Three Evil Forces, while it has emphasised on upholding sovereignty and territorial integrity. Terrorism has moved into the cyberspace and has been using it as a safe haven for planning terrorist attacks. This space enables terrorists to easily find and target political, social, or religious objectives.[31] China has 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.[32] Further, China has very cautiously and carefully restricted several social networking sites, forums, chat rooms, and other social interactive platforms to prevent the spread of erroneous thoughts of separatism and extremism which could corrupt the communist ideology and threaten the security of China. The religious movement of Falun Gong can be taken as an example where internet had been deemed to be central to the growth of the movement and significant in bringing pressure against the Chinese government, particularly at the international level. Founded by Li Hongzhi as a spiritual discipline in 1992, the movement's growth threatened the CPC's authority and the undivided loyalty of the citizens towards the government. As a result, in 1996, the government banned the public sales of the movement's main text known as 'Zhuan Falun', while newspaper editorials started attacking the movement, claiming the Falun Gong to have ill-effects on the adherents.[33]

Consequently, in April 1999, more than 10,000 indignant Falun Gong practitioners staged a protest outside Zhongnanhai - CPC's headquarters in Beijing - which lead the government to seek to suppress the movement and declare the sect as illegal in the following month.[34] Importantly, the Falun Gong used the internet to organise activities and pass on information in and outside the country, which played an important role in enabling the practitioners to stage protests, such as the one outside Zhongnanhai. Primarily, the internet was crucial for the adherents to stage mass demonstrations and individual protests and continue their struggle against the Chinese government, even after the sect was banned, and widespread arrests and intimidations were prevalent.[35]

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, 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: (a) national security and domestic stability, (b) preserving the rule of the CPC, and (c) facilitating economic growth.[36] Article 35 of the Constitution allows the people of China the fundamental freedoms of speech, press, association, demonstration and procession. [37] However, articles in State Council Order No. 292, particularly under article 15, promulgated in September 2000, gives guidance on content restriction for internet content providers, disallowing them from disseminating information which goes against the constitution; endangers the national security; leaks state secrets; undermines the state power and national unity.[38] The above contradiction shows the opacity of Chinese internet regulations which allows the authorities to crack down on any content which exposes state secrets, and thus threatens the security of the country.[39] Notably, the term 'state secrets' has vaguely been described by the Chinese government; they can be argued to be any information which is deemed harmful to the authorities on account of being directed against the government, possibly leading to the downfall of the regime.[40]

In hindsight, China has been controlling public information since the 1950s. Post-Tiananmen Square incident in 1989, tighter controls over the masses were initiated. The same can be applied to the internet governance in China where the government exercised stringent controls over the content flow to ensure the preservation of the state security and the public order; to uphold socialist and communist ideals; and sustain the legitimacy of the CPC. Importantly, China, which entered the cyberspace relatively later than many advanced countries, acknowledged the openness and limitlessness of the domain. Accordingly, the CPC also sensed the implications of the domain for its control over the masses. Thus, the Chinese government, throughout the later decades of the 20th century and till the current times, has been manoeuvring between the need for advanced technology for higher economic growth and the requirement for prevention of polluting the state ideals through erroneous influences. The correct balance between both has been a defensive strategy to ensure a stable cyberspace for 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. The Cyberspace has also become factored with censorship against the content on the internet, which goes against the government's laws. 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, published in 2010 by the State Council.[41] 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 organisation under the UN system through democratic procedures on a worldwide scale'.*[42]

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.[43] 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 cyber environment.[44] However, the element of ambivalence was manifested through China's Cybersecurity Law passed in 2016 and implemented in June 2017, which linked distinct sovereignties to different countries.[45] According to the document, every country has its own perception of sovereignty, and irrespective of the cyberspace being a global arena, how a country should govern the cyberspace should be subjected to the respective country's jurisdiction.

Hence, according to these documents, China recognises the open and democratic procedures of the cyberspace and has no qualms in administering the domain according to the United Nations (UN) system. However, it also believes in the concept of freedom to adjudicate the cyberspace according to its own will and apply rules and regulations wherever it deems necessary. Thus, 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.*[46]

This 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 its national security. Cyber sovereignty, hence, becomes a defensive 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 unravelled 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 secure and stable development of technology.[47] 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 CPC 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 Chinese, as well as foreign companies based in China to comply with investigative measures under the garbs of national security.[48]

Military Defences

The application of information technology in the military domain is imperative to safeguard China's national security.[49] A reiteration of this took place in 2015 when the Information Office of the State Council published a white paper on China's military strategy, which, notably, addressed cyber warfare more comprehensively, as it stated:

> *'Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces… As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability.*[50]*'*

The document echoed China's acknowledgement of the existence of cyber-attacks and its potential. It also stressed on the necessity to prepare the People's Liberation Army (PLA) to deter such attacks, which remains potent for China's security and development. China is currently strengthening the PLA Strategic Support Force (PLASSF) as being integral to PLA's objectives of fighting and winning "informatized" warfare. Further, its network systems department has been combining 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.[51] Further, the centralised command and control systems using integrated information and firepower can aggrandise China's military cyber power.[52] However, for PLA, coordinating information across the various units as well as synchronising warfare capabilities remains the primary test, especially under the newly formed theatre commands.

Moreover, the Central Military–Civil Fusion Development Commission's formalised Cyberspace Security Military–Civil Fusion Innovation Centre, which is being led by Xi Jinping himself, is aiming at national cyber defences.[53] Set up under the instruction of the Central Commission for Integrated Military and Civilian Department and related military bodies, the centre seeks to establish cutting-edge cyber security defense system, contributing towards building the PLA's capability to win future wars.[54] The initiatives mentioned above reverberate the military aspect in China's cyber governance, only to enhance the strategic underpinnings.

Implications of China's Cyber Sovereignty on Society

Considering the cyber defensive strategies of China, it is essential to understand its implications on the Chinese 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 the internet content accessible to its population. [55] Further, its science and the technology sector is developing under China's nationalist approach.[56] While these policies have been highly successful in an economic forum, these are not existent without considerable costs. As per the UN, extensive control over internet or forbidding access to the internet is a violation of human rights.[57] It is essential to note that China itself promotes cooperation with the international community and encourages establishment a universally accepted internet administrative organisation under the UN system.[58] However, China's internet governance shaped by information control has not just received extensive international criticisms but has also witnessed domestic despair.

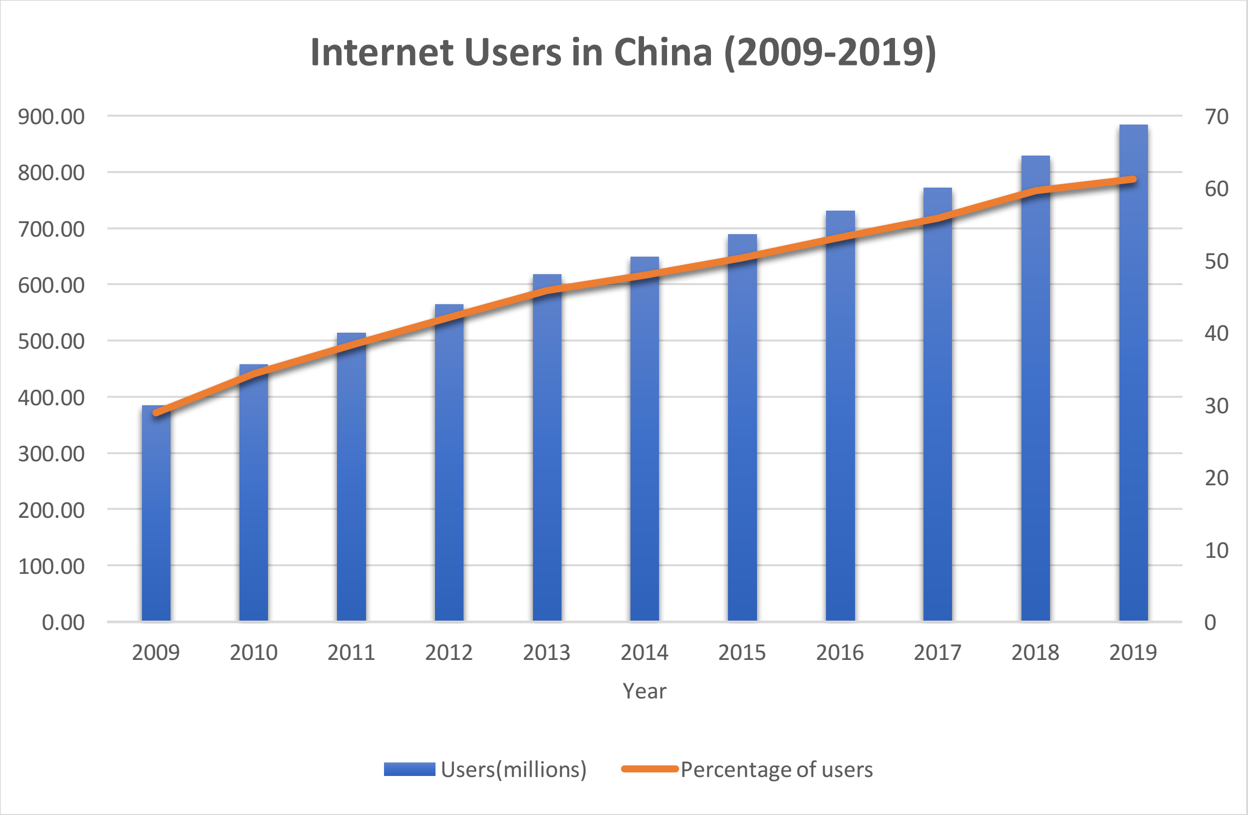
Given the stringent restrictions on internet content access, VPNs were the only source to access open information for people in China and circumvent the Great Firewall.[59] These were sources through which people could evade the censorship and access restricted websites with basic facilities such as emails and web search. The government, however, in an unprecedented policy move, instructed the telecommunication carriers to regulate access to VPNs.[60] The regulation on VPNs shut down the only window open for the people of China to access the contents beyond the ones allowed by the government. This step allowed the CPC to have better control over the population by using regulations to reprimand people who build or use VPNs. The regulations were 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.[61] These have been having unfavourable implications, especially on the people without any marked detrimental intent towards the government or the country.[62]

However, the masses in China have used technological as well as linguistic creativity to circumvent the Firewall in China. While the government of China shut down the VPNs, there are still several ones such as Astrill, ExpressVPN, Hotspot Shield, ibVPN, Ivacy and more which have been enabling masses to access blocked and censored websites and contents.[63] 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.

Further, censorship by the government demonstrates that China expects its citizens to be as apolitical as possible for the seamless 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 substituting 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 characterised by heavy censorship; and the *River Crab* which similarly denotes the Chinese government's policies of censorship.[64] 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.[65] This book, later on, was 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 internet as a medium.

Figure 1: Internet users in China



Source: China Internet Network Information Center (www.cnnic.com.cn)

The above figure demonstrates the increasing percentage of people using the internet and the subsequent growth in internet traffic in China. The figure reverberates 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 significant level, and the internet control by the government is becoming counter-productive. However, an explanation for this development can also be the government's successful generation of attractive alternatives to western technology by innovating its own technology.

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 is enabling the rise of Baidu, WeChat, TikTok and more which, in fact, in the view of current developments, are successfully competing with their Western counterparts.[66] 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 key part of this argument. The above demonstrates the internet to be as significant to the Chinese government as it is for the Chinese society to diffuse their opinion. The above argument further reiterates how the Chinese government considers the internet space as a medium to enhance the party legitimacy by influencing people through its propaganda tactics, rather than a limit to CPC's governance.

Offensive Strategy to Offset Cyber Attacks

Recognising the growing threats in the cyberspace amidst 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 ICT platform which would have the capabilities to command at levels of informatisation, strategic planning and training services. [67] The Cyberspace is further being explored to be used for strengthening the PLA activities.[68] Such a link between the cyber and military domains was first established in a document released by China's Academy of Military Science in 2013, titled 'The Science of Military Strategy'.[69] 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 with Chinese origins.[70] Similar allegations were reported by Canada and even the Dalai Lama whose computer systems were attacked by a large-scale electronic espionage program known as Ghost-Net.[71] Subsequently, systems of Google Inc, Adobe Systems Inc and several other companies were also attacked by a targeted malware called Aurora, which aimed to access other systems of the US corporations.

Further, in 2012, the National Security Agency of the United States, after investigations, accused China of cyber espionage and stealing intellectual property.[72] The study further attributed to China for an attack on the systems of the RSA, the previous year, which were of national importance and dealt with classified work for the Pentagon.[73] As per the investigation report, these attacks were spear-phishing attacks[74] aimed at benefitting the R&D in China by understanding the workings of a system under attack and comprehend the entry points to the system. At present, such cyber developments have been relatively common between the US and China, pushing them to the verge of an escalation. In fact, the cyber tensions between the US and China are classic examples to understand the US-China relations in terms of the global competition, on the one hand, and the perilous workings of cyberspace on the other.

The US Factor in China's Cyber Governance

The reasons to control the internet space for China go beyond national security towards theoretical aspects. Significantly, China, as a country embracing the cyberspace relatively late in 1994, looks at the arena through the lens of technological inequality and Neo-Realism.[75] The general argument put forward is that the low restrictions and institutionalisation 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. This proved disadvantageous for the developing and the underdeveloped nations, while the technologically advanced – mainly the west – monopolised the space in accordance with their benefits and used the internet as a tool for their diplomacy. This was perceived as highly detrimental by China, especially for its developing economy.[76] Thus, for China, cyber sovereignty became a tool for the sustenance of its national development and a medium to protect its interests at the face of the US using the internet to expand its influence and exercise its power. Essentially, China does not trust the multi-stakeholder model of internet governance, favouring certain countries which exploit the advantages of ICT.[77] For this reason, China would want to reform the global cyber structure; this sentiment has witnessed greater emphasis under Xi Jinping.

Xi, in his remarks at the opening of the World Internet Conference at Wuzhen on 16 December 2015, emphasised on the "transformation of the global internet governance system" through four principles: Respect for cyber sovereignty; Maintenance of peace and security; Promotion of openness and cooperation; and Cultivation of good order.[78] Further, Xi, at the national conference on the work of cybersecurity and informatisation, held from 20-21 April 2018, stressed on the prevalence of the common aspiration of the Chinese people to promote the reformation of the global cyberspace governance.[79] The reform would take place by adopting a multilateral approach with multi-party participation from the government, international organisations, internet enterprises, technology communities, non-governmental institutions, and individuals. These events, if anything, reverberated a unilateral approach by China to gradually reform the international cyber domain, so as to attain its core strategic goal of global acceptance of its values and interests.

However, the US, particularly under Donald Trump, has viewed China's unilateral objectives through a confrontational approach, which was prevalent as Washington, in its National Defense Strategy of 2018, proclaimed China as a 'revisionist' country.[80] Further, the US has been condemning China's nonchalant approach towards human rights and its failure to manoeuvre within the gambits of the cyber standards set by international institutions. Essentially, the US' report by the Economic and Security Review Commission in 2018 to the US Congress had compiled many cases where cyber threats with Chinese origins had tried to attack systems of critical infrastructures or devices carrying information related to state security.[81] Subsequently, the US had accused China of violating an agreement that was signed by the then president of the United States, Barack Obama and the General Secretary of China, Xi Jinping in 2015.[82] 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 cyber crime through a joint high-level dialogue mechanism.[83] However, Trump accused China of violating the agreement in 2018,[84] particularly in accordance with reports released by the US government in 2014, highlighting $300 billion worth of cyber espionage committed by China.[85] While the numbers did decline post the agreement in 2015, US reports still recorded considerable amounts of cyber espionage by China thereafter.[86]

Thus, in May 2019, Donald Trump banned Huawei from dealing with US companies in his 'Executive Order on Securing the Information and Communications Technology Services Supply Chain'.[87] 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. Notably, the CPC's significant command over Chinese private companies and 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.[88] This, when viewed, keeping in mind the functionality of China's National Intelligence Law, only make matters more complicated.

The US and many other countries, in this context, have started to acknowledge the strategic underpinnings of doing business with Huawei, and have been disallowing the company to participate in their 5G trials.[89] This comes from a developing perception amongst several countries regarding the Chinese companies such as Huawei being actors of an authoritarian state, carrying values of unilateralism, opaqueness and revisionist desires.[90] Further, China's cyber governance has been condemned by the US, which tries to ensure a 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.*[91]

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.*[92]

The above statements reiterate the US perception of cyber security which remains as much offensive as defensive. Its cyber strategy, emphasising on 'Persistent engagement' and 'defend forward' becomes an initiative to secure itself from cyber attacks, especially from the state-sponsored ones.[93] 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 the US and Iran between 2019-2020.[94] 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.[95] Importantly, this reiterated a covert and 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.[96] China has instead accused the US of carrying out its political agenda by placing allegations against Washington. It has stated:

> *For a long time, relevant US government departments have instigated large-scale, organised online hacking activities against foreign governments, companies, and individuals.*[97]

Articles in Chinese newspapers, such as *Global Daily*, have also criticised the US for exercising prejudiced and threatening levels of influence over the global cyber domain through the Internet

Corporation for Assigned Names and Numbers (ICANN).[98] On the contrary, it should be noted that the US cannot control the internet, even if the ICANN governance system originates from the US.[99] This statement, while indicating China's defensive approach towards tech politics with the US, also demonstrates the underpinning assertiveness in its diplomacy in preserving its technological advancement and economic growth. A factor towards China's defensive approach can be argued as the importance of 'prestige' and 'dignity' in Chinese culture denoted by the terms *Lian* and *mianzi.*[100] The former term focuses on a "sense of shame in relation to social standards of morality and behaviour". The latter, *mianzi*, concentrates on "status, prestige and social position". These demonstrate the importance of the 'face' in the Chinese culture, which is considered far more psychological than physiological. It can be argued that the public image remains of the utmost importance for China. It would portray itself as a nation which believes in the concept of 'peaceful rise' and seeks harmony. Another explanation for this remains what Sun Zu described as an essential art of war- to 'subdue the enemy without fighting'.[101] Essentially, 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.' [102] These three strategies were:

Psychological Warfare–Undermines an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralising 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.

China uses these strategies to mould a tensed situation according to its interests in such a way that its activities or reactions are not questionable in the domestic or international domain.

In brief, China, through its cyber sovereignty, has been seeking to alter the course of the cyber content according to its own will in the domestic arena to ensure the legitimacy of the CPC. At the same time, it focuses on acquiring information as a foundation for its cybersecurity and as a defensive strategy.[103] These, coupled with China's desire to reform the cyberspace, has been creating apprehensions for many countries, especially as the strategic and security bearings of Beijing's cyber laws and policies become more overt. The governance is also being explicitly and firmly condemned by the US; which, in the backdrop of an intensifying economic and strategic competition between both the countries, is pushing Beijing and Washington towards a cyber conflict. Weighing these developments taking place simultaneously, greater challenges for Xi Jinping and the CPC's objective to transform China into a strong cyber power remain inevitable.

China's Cyber Governance and the Covid-19 Pandemic

Even though the CPC under the guidance of Xi Jinping has been controlling the information flow through its policies shaped 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 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 medical professionals and scientists 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 the country, 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.[104] 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 public outrage.[105] 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 in the online domain 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 in Hong Kong and a significant amount of protests from the international community, particularly by the US tech giants.[106] 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 to China, remains the current powers of the city's Chief Executive- a pro-Beijing appointee- to approve applications for interception and covert surveillance operations. This development undoubtedly has grave repercussions for the security of the people of Hong Kong, as well as the international community connected to the region; thus, having global consequences.[107]

Even as China's control over the internet and its surveillance network seem formidable, the significant amount of resistance and criticisms in and outside China, respectively, 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 after the COVID-19 episode, creating greater challenges for the CPC and Xi.

Conclusion

This paper, from the means of evaluating China's approach to the 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 only strengthened its techno-capabilities. Through the same argument, the paper linked China's domestic scenario with the friction it is witnessing in the international forum. Undoubtedly, China's intent to regulate the information flow inside its territory and desire to reform the cyberspace in the global arena 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 more significant challenges. Further, the international community is gradually becoming active in criticising China's questionable cyber policies and activities, which, to a certain extent, would affect the CPC's international standing and China's global governance under Xi Jinping.

Endnotes

[1] The term 'multi-stakeholder governance' came into use around 2004. It can be largely defined as a tool for policy dialogue where all the stakeholders can participate on an "equal footing" towards global decision-making, through an open, inclusive and transparent process. Please read, Marcus Kummer, 'Multi-Stakeholder Initiatives: A Strategic Guide for Civil Society Organisations, The Social Science Research Network', *Internet Society*, 14 May 2013, https://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-on-the-emergence-of-a-new-phraseology-in-international-cooperation/ (accessed September 6, 2019). Notably, at the World Conference on International Telecommunications held in December 2012, the members of the United Nations International Telecommunication Union (ITU) remained fragmented and were unable to reach a consensus over the approach to follow for internet governance. While the US and its key allies advocated for a multi-stakeholder model of governance, claiming the model to have the capabilities required to counter the global internet policy challenges, several countries advocated for greater governmental control over the internet, resulting in a stalemate. Subsequently, the Global Multistakeholder Meeting on the Future of Internet Governance was convened in Brazil in April 2014, which concluded with a nonbinding statement in favour of consensus-based decision making, where countries including Russia, China and Iran favoured a multi-lateral model of governance over a multi-stakeholder model. Please see, Stuart N. Brotman, 'Multistakeholder Internet governance: A pathway completed, the road ahead', *Center for Technology Innovation at Brookings*, July 2015, https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder-1.pdf (accessed on 6 September 2019); John E. Savage and Bruce W. McConnell, 'Exploring Multi-Stakeholder Internet Governance', *EastWest Institute*, January 2015, https://www.eastwest.ngo/sites/default/files/Exploring%20Multi-Stakeholder%20Internet%20Governance_0.pdf (accessed on 6 September 2019).

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

[3] 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

[4] The enhancement of science and technology was a necessary instrumentality of Deng Xiaoping's Thought, which led the Deng's era to depart from Maoism. Deng identified science and technology as a "primary" productive force; the advancement of which would lead the Chinese economy

towards "rapid development". Deng focussed on technical transformation and scientific experimentation through the extensive application of advanced science and technology to industry and agriculture to ensure "greater, faster, better and more economical growth". Please read, Deng Xiaoping, 'Speech at the opening ceremony of the national conference on science', *China Daily*, March 18, 1978, http://cpcchina.chinadaily.com.cn/2010-10/15/content_13918179.htm (accessed on 6 September 2019); Maria Hsia Chang, 'The Thought of Deng Xiaoping', *Communist and Post-Communist Studies*, Vol. XXIX, No. 4, 1996, 387.

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

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

[7] 'Full text of Hu Jintao's report delivered at the 17th National Congress of the Communist Party of China (CPC) on Oct. 15, 2007', *China Daily*, 15 October 2007, https://www.chinadaily.com.cn/china/2007-10/24/content_6204564.htm (Accessed on 3 November 2019)

[8] 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*, Volume VIII, No. 1 October 2008, https://pdfs.semanticscholar.org/d8ce/036ab6a23051b2244a34f5cf70455270f421.pdf (accessed on 6 September 2019).

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

[10] 'Full text of Hu Jintao's report at 18th Party Congress', *Embassy of the People's Republic of China in the United States of America*, 27 November 2011, http://www.china-embassy.org/eng/zt/18th_CPC_National_Congress_Eng/t992917.htm. (Accessed on 20 August 2020)

[11]China's GDP per capita as of 2019 was $10,276, which was though growing at a considerable rate, was 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*, 17 January 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 20 August 2020)

[12] The CNP could be defined as the combined weight of economic, diplomatic and military power. From a state-centric perspective, sustained growth in CNP 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.

[13] 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*, 18 October 2017, https://mp.weixin.qq.com/s/EpdgYurAxZ2bnKZnZuenfg (accessed on 6 September 2019).

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

[15] 'Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road', *National Development and Reform Commission (NDRC)*, People's Republic of China, 28 March 2015, https://en.ndrc.gov.cn/newsrelease_8232/201503/t20150330_1193900.html. (Accessed on 3 November 2019)

[16]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, 05 March 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, 96-106.

[17] While China's regulatory model of cyber governance is being questioned by many countries, China's technology infrastructural initiatives such as the Digital Silk Road might remain feasible in an environment where resources are more constrained, particularly with the onset of the COVID-19. In such a scenario, China's DSR might witness a relatively easy and deeper access into emerging markets. Jude Blanchette and Jonathan E. Hillman, 'China's Digital Silk Road after the Coronavirus', *Center for Strategic & International Studies*, 13 April 2020, https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus (Accessed on 23 August 2020); Robert Greene and Paul Triolo, 'Will China Control the Global Internet Via its Digital Silk Road', *Carnegie Endowment for International Peace*, 08 May 2020, https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857. (Accessed on 23 August 2020)

[18]Please read, 'Full text of Xi Jinping's report at 19th CPC National Congress', *China Daily*, 04 November 2017, https://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm. (Accessed on 3 November 2019)

[19]Please read, Rogier Creemers. 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.

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

[21] 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 surveil the internet. Other techniques involve limiting access to undesired websites and shutting them down. Importantly, trying to evade the Great Firewall comes with legal consequences, leading up to detainment of 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.

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

[23] Ekaterina Stepanova, 'The Role of Information Communication Technologies in the "Arab Spring": Implications beyond the region', *PONARS Eurasia*, Policy Memo No. 9, 1, http://pircenter.org/kosdata/page_doc/p2594_2.pdf. (Accessed on 23 August 2020)

[24]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, 2015, 105-135

[25]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*, 19 May 2016, https://www.scmp.com/news/china/policies-politics/article/1947376/revealed-digital-army-making-hundreds-millions-social. (Accessed on 23 August 2020)

[26]According to a report by Statista titled "Most valuable technology brands worldwide in 2020" released on 15 July 2020, Chinese companies such as Tencent, Huawei, Baidu, and Xiaomi hold the top positions globally. In fact, Tencent holds 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. While the 5G technology is turning into a battleground between the US and China, Huawei might have proven to be the Trojan horse for China to enhance its global technological footprints and power. Thomas Alsop, 'Most valuable technology brands worldwide in 2020', *Statista*, 15 July 2020, https://www.statista.com/statistics/267966/brand-values-of-the-most-valuable-technology-brands-in-the-world/. (Accessed on 24 August 2020); Keith Johnson and Elias Groll, 'The Improbable Rise of Huawei', *Foreign Policy*, 03 April 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/. (Accessed on 24 August 2020)

[27] 'China has 854 mln internet users: report', *Xinhua*, August 30, 2019, http://www.xinhuanet.com/english/2019-08/30/c_138351278.htm (accessed on 7 September 2019).

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

[29]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*, 8 February 2020, https://www.project-syndicate.org/commentary/coronavirus-will-not-change-xi-jinping-china-governance-by-kevin-rudd-2020-02 (accessed on 7 April 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*, 8 July 2019, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1679454.shtml (accessed on 7 April 2020); 'Full Text: China's National Defense in the New Era', *Xinhua*, 24 July 2019, http://www.xinhuanet.com/english/2019-07/24/c_138253389.htm (accessed on 7 April 2020).

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

[31] '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, 21 March 2012, 110–123

[32] Catherine Wong Tsoi-lai, 'Conference calls for global effort to combat cyber terror', *Global Times*, 21 November 2014, https://www.globaltimes.cn/content/892929.shtml (accessed on 6 September 2019).

[33] 'What is Falun Gong?: China calls it an "evil cult", *The Economist*, 5 September 2018, https://www.economist.com/the-economist-explains/2018/09/05/what-is-falun-gong. (accessed on 6 September 2019).

[34] 'Senior CPC Official on Falun Gong Prohibition', *People's Daily*, 24 July 1999, http://en.people.cn/special/fagong/1999072400A104.html. (accessed on 6 September 2019).

[35] Mark R. Bell and Taylor C. Boas, 'Falun Gong and the Internet: Evangelism, Community, and Struggle for Survival', *Nova Religio*, Volume VI, No. 2, 2003, 283-287.

[36] 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.

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

[38] Premier Zhu Rongji, 'Measures for the Management of Internet Information Services', *Chinese Law and Government,* Volume XXXXIII, No. 5, Septembe-October 2010, 33

[39] Beina Xu and Eleaor Albert, 'Media Censorship in China', *Council on Foreign Relations*, 17 February 2017, https://www.cfr.org/backgrounder/media-censorship-china (accessed on 6 September 2019).

[40] Please read 'State Secrets: China's Legal Labyrinth', *Human Rights in China*, 2007, https://www.hrichina.org/sites/default/files/publication_pdfs/hric_statesecrets-report.pdf (accessed on 6 September 2019).

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

[42] Ibid.

[43] '2013 China Diplomatic White Paper: China's determination to maintain territorial sovereignty is firm (reproduced)', *People's Daily Online*, 17 July 2013, http://bbs.tianya.cn/post-worldlook-827386-1.shtml (accessed on 6 September 2019).

[44] Please read, Severene Arsrene, 'Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic Order?' *China Perspectives*, Volume 2, No. 106, 2016, 25-35

[45] Ibid.

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

[47] '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*, 27 June 2017, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (Accessed on 23 August 2020); Bonnie Girard, 'The Real Danger of China's National Intelligence Law', *The Diplomat*, 23 February 2019, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/ (Accessed on 23 August 2020)

[48] Lauren Maranto, 'Who Benefits from China's Cybersecurity Laws?', *Center for Strategic and International Studies (CSIS)*, 25 June 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 23 August 2020)

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

[50] ‘China’s Military Strategy’, *The State Council Information Office of the People’s Republic of China*, 27 May 2015, http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm. (Accessed on 23 August 2020)

[51] Elsa B. Kania & John Costello, ‘Seizing the commanding heights: the PLA Strategic Support Force in Chinese military power’, *Journal of Strategic Studies*, Volume XXXXIII, No. 4, May 2020, 9.

[52] Ibid.

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

[54] Ibid.

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

[56] Simon Hansen, ‘Techno-nationalism in China’s rise: the next gunpowder moment’, *The Strategist*, Australian Strategic Policy Institute (ASPI), 14 October 2014, https://www.aspistrategist.org.au/techno-nationalism-in-chinas-rise-the-next-gunpowder-moment/ (accessed on 7 September 2019).

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

[58] ‘Position Paper of the People’s Republic of China For the 73rd Session of the United Nations General Assembly’, Ministry of Foreign Affairs of People’s Republic of China (fmprc), 28 August 2018, https://www.fmprc.gov.cn/mfa_eng/wjbxw/P020180828720627338850.pdf. (Accessed on 23 August 2020); Nina Hachigian, “China’s Cyber Strategy”, *Foreign Affairs,* Volume LXXX, No. 2, March-April 2001, 123–128.

[59] Virtual Private Network (VPN) are networks that are capable of circumventing the restrictions and censorships by the government on internet content. It provides encryption between a person’s device and the broader internet, such that the communications are not subjected to interception. For more information, please see Jay Adkisson, ‘Why You Need a Virtual Private Network’, *Forbes*, 19 October 2018, https://www.forbes.com/sites/jayadkisson/2018/10/19/why-you-need-a-virtual-private-network-vpn/#201436de3a31 (accessed on 7 September 2019);

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 on 7 September 2019); Alexander Chipman Koty, 'Why HR Should Care about VPN Use in China', *China Briefing*, 21 June 2018, https://www.china-briefing.com/news/vpn-china-hr-due-diligence/. (accessed on 7 September 2019)

[60] 'China tells Carriers to Block Access to Personal VPNs by February,' *Bloomberg News*, 11 July 2017, https://www.bloomberg.com/news/articles/2017-07-10/china-is-said-to-order-carriers-to-bar-personal-vpns-by-february (accessed on 23 August 2020)

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

[62] Ibid.

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

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

[65] '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 3 November 2019)

[66] Please refer to endnote no. 26.

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

[68] Please read, 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.

[69] The Academy of Military Science, no. 67.

[70] Nigel Inkster, no. 67.

[71] The Ghost-Net electronic espionage program was used to spy on individuals, organizations and government, breaching approximately 1295 computers and103 countries over a span of two years. This operation was discovered after an investigation into a potential breach of the office of

the Dalai Lama, residing in India. Investigation at the University of Toronto confirmed that the threats originated from China. John Markoff, 'Vast Spy Systems Loots Computers in 103 Countries', *The New York Times*, 28 March 2009, https://www.nytimes.com/2009/03/29/technology/29spy.htm (accessed on 7 September 2019).

[72] Colin Clark, 'China Attacked Internet Security Company RSA, Cyber Commander Tells SASC', *Breaking defense*, 27 March 2012, https://breakingdefense.com/2012/03/china-attacked-internet-security-company-rsa-cyber-commander-te/ (accessed on 7 September 2019).

[73] Ibid.

[74] Spear-phishing attacks are attacks towards an individual or a group of computers which is carried out by sending emails to targeted systems. Once attacked, the virus, such as the Trojan malware, 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*, 13 April 2019, https://www.cyberdefensemagazine.com/the-impact-of-usability-on-phishing-prevention-effectiveness/ (accessed on 7 September 2019).

[75]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 the trust factor, 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.

[76] Ibid.

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

[78] 'Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference', *Ministry of Foreign Affairs of the People's Republic of China*, December 16, 2015, https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (accessed on 7 September 2019).

[79] 'Xi outlines blueprint to develop China's strength in cyberspace', *Xinhua*, 4 April 2018, http://www.xinhuanet.com/english/2018-04/21/c_137127374_2.htm (accessed on 7 September 2019).

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

[81] 'Report to Congress of the US-China Economic and Security Review Commission, 2018', *USCC 2018 Annual Report*, 2 November 2018,

at https://www.uscc.gov/sites/default/files/annual_reports/2018%20Annual%20Report%20to%20Congress.pdf (accessed on 7 September 2019).

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

[83] Ibid.

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

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

[86] '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 on 7 September 2019).

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

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

[89]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*, 14 July 2020, https://mr.usembassy.gov/welcoming-the-united-kingdom-decision-to-prohibit-huawei-from-5g-networks/. (Accessed on 20 August 2020); Joe Panettieri, 'Huawei: Banned and Permitted in Which Countries? List and FAQ', *Channele2e*, 20 August 2020, https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/. (Accessed on 20 August 2020)

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

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

[92] Ibid.

[93] Please read, 'Jason Healey, The implications of persistent (and permanent) engagement in cyberspace', *The Journal of Cybersecurity,* Volume V, No. 1, 2009, 1-15.

[94] Julian E. Barnes, ' U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say', *The New York Times*, 28 August 2019, https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html (Accessed on 3 November 2019)

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

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

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

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

[99] 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.

[100] Please read, Aris Teon, 'The Concept of Face in Chinese Culture and the Difference Between Mianzi and Lian', *The Greater China Journal*, 25 February 2017, https://china-journal.org/2017/02/25/the-concept-of-face-in-chinese-culture-and-the-difference-between-mianzi-and-lian/#:~:text=Broadly%20speaking%2C%20lian%20means%20%E2%80%9Csense,%2C%20prestige%2C%20social%20position%E2%80%9D (accessed on 7 September 2019).

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

[102] '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 on 7 September 2019).

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

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

[105] Kuang Biao, ‘China’s coronavirus cover-up: how censorship and propaganda obstructed the truth’, *The Conversation*, 7 March 2020, https://theconversation.com/chinas-coronavirus-cover-up-how-censorship-and-propaganda-obstructed-the-truth-133095. (Accessed on 20 August 2020)

[106] Ahence France-Presse, ‘China censors internet in Hong Kong’, *The Hindu*, 7 July 2020, https://www.thehindu.com/news/international/china-censors-internet-in-hong-kong/article32015853.ece (Accessed on 20 August 2020)

[107] Steven Feldstein, ‘China’s Latest Crackdown in Hong Kong Will Have Global Consequences’, *Carnegie Endowment for International Peace,* 9 July 2020, https://carnegieendowment.org/2020/07/09/china-s-latest-crackdown-in-hong-kong-will-have-global-consequences-pub-82264. (Accessed on 20 August 2020)

…………………………………………………………………………………………………

This paper was presented at AICCS, 2019

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.

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