Contemporary Chinese Political Economy and Strategic Relations: An International Journal Vol. 7, No. 2, August 2021, pp. 691-715

Fragmenting Cyberspace and Constructing Cyber Norms: China's Efforts to Reshape Global Cyber Governance[+]

Hon-min **Yau**[*]
National Defense University, Taiwan

Abstract

Digitalisation has been an essential element behind the process of globalization, proposing new ways of interacting among nations and states. With its rise in the digital domain, China has increased its involvement in the global dialogue regarding cyber governance. China has sought to achieve a position from which it is capable of reshaping the global digital domain as dictated by its interests. This endeavour into cyberspace leadership entails not only technological but also political transitions. Hence, this article explores China's attempts to dictate the future direction of cyber norms and investigates this process of discursive production in an effort to understand how China may expand its influence, reshape the expectations of international audiences, and establish a favourable strategic environment by "telling China's stories well". The investigation concludes by discussing the implications for the international community and cyberspace.

Keywords: *discourse power, global cyber governance, cyber norms, data governance, cyber sovereignty*

1. Introduction

Since the first email was sent from China on the 20th September 1987, containing the message "Beyond the Great Wall, joining the world" (Qiu, 2003), China has developed a considerable presence in cyberspace. After decades of digitalisation, in 2016, China became the country with the largest population of Internet users and a quickly expanding cyber market (*Internet Live Stats*, 2016). In addition, Chinese homegrown technology now occupies a sizeable share of the global technology market, and various domestic companies such as Baidu, Youku, Taobao, Alipay, Weibo, and Renren are capable of rivalling Google, Youtube, eBay, PayPal, Twitter, and Facebook (Yau, 2019: 277). In sum, China has invested substantially to become a formidable cyber power in the 21st century.

Nevertheless, China's aspirations in cyberspace are both materialistic and ideological. Existing research often placed their focus on understanding the roles of the tech sector in China's growth of power in cyberspace, but they sometimes ignored the contested relations between the state and the private sector and simplified them as a coherent group. As exemplified by China's interventions on the Alibaba Ant Group's expansion in the market and removal of Chinese DiDi from the domestic app store in 2021 (*Taiwan News*, 6th July 2021; *Financial Times*, 23rd April 2021), the Chinese Communist Party (CCP) would rein the direction of technology whenever the party feels the interest of the private sector is incompatible with its domestic policy of cyber governance. Likewise, internationally China would also seek not only the enhancement of technology but a new strategic position in which it

can make the rules rather than a subordinate position in which it must accept rules made by others. This observation has become increasingly evident since Xi Jinping assumed the presidency of China and the position of General Secretary of the CCP in 2012. In July 2014, President Xi Jinping officially called for countries to respect each other's cyber sovereignty during a visit to Brazil (*China Daily USA*, 17th July 2014), reiterating the point at China's 2015 World Internet Conference (Xinhua, 16th December 2015). By the end of 2019, what is also noticeable is that China and its close ally, Russia, had successfully mobilised sufficient international support to establish a new United Nations (UN) working group, the Open-Ended Working Group (OEWG), with a stated goal to "enrich and elaborate" how the principle of sovereignty applies in cyberspace (United Nations, 2019: 2). China contends that cyberspace requires strict order and promotes a state-centric view of the digital domain, which is at odds with the conventional Western idea of a borderless cyberspace.

Based on this context, this article explores China's efforts to intervene in global digitalisation with respect to ideology. In particular, the investigation focuses on how China has reshaped the existing discussions and focuses on cyber governance. The study is structured as follows. First, it explains the division between the East and West in regard to cyber governance through a brief review of the main points of contention. Second, the paper highlights how its analytical approach is distinct from previous research. Third, it explains how discourse is meaningful and why narratives are crucial to the development of cyber norms. Fourth, it revisits the historical use of discourse in the shaping of cyber norms. Fifth, the study presents the evidence of Xi's focus on creating a strategy to guide cyber norms. Sixth, the article delves into how China has exerted power within UN discussions and debates and the dynamics of its participation. Finally, the paper describes the

implications of the analysis and how China's carefully crafted cyber vision may have broader security ramifications for the world.

2. The Debate on Cyber Governance

China's narratives concerning cyber sovereignty reflect a long-standing dispute between the East and the West regarding cyber governance, or how to regulate behaviour in cyberspace. They both acknowledge the need to develop agreeable new cyber norms to regulate conduct in cyberspace and prevent the World Wide Web from becoming a "Wild West Web" (Arquilla and Ronfeldt (eds.), 1997: 242); however, due to differences in their political systems and cultures, East and West have arrived at distinct interpretations of the state's role in cyberspace (Lu, 2014). As promoted by the United States, the West supports a model of "multi-stakeholder governance". Western countries argue that because cyberspace infrastructure is constructed, managed, operated, and supported by the private sector, no government may act alone to address cyberspace issues. Instead, individuals, the Internet community, enterprises, nongovernmental organizations, and governments should all be involved in cyber governance through proper coordination and cooperation. However, led by China and Russia, the East insists on a model of "multilateral governance". They argue that cyber "governance" is not distinct from cyber "government", And that that the international community should follow the UN's state-centric tradition to regulate this new domain, and that the International Telecommunication Union under the UN should steer cyber governance affairs. For China, the discourse on "multilateral governance" should been repackaged as "cyber sovereignty". According to China's official announcement upon the establishment of the OEWG in 2019, states should "exercise jurisdiction" over information and communication technology (ICT)

infrastructure and ICT-related activities within their territories and states "have the right to make ICTs-related public policies" to manage their own ICT affairs and protect their citizens in cyberspace (United Nations, 2019: 3). From this perspective, cyber governance encompasses not only technological responsibility but also social and policy aspects relating to ICT infrastructure; China is determined to make cyber sovereignty a legitimate cyber norm.

3. The Research Question

The context presented above indicated that cyber norms are still agreements yet to come, and it would be too early to say, in Marxism terminologies, whether China's waging of a *war of position* would enable it to complete in a *passive revolution* in changing our view of cyber governance under Xi Jinping's leadership. However, the research question presented here is that, technically speaking since China was a relative latecomer in the ICT area at the beginning of the 21st century, how has the country been able to transform itself from a position of dependency towards potentially having a dominant status, by overcoming the West's past technological superiority in the tech sector?

To answer this question, this paper adopts the premise that the future of cyber governance will not be decided by who has more technology but by who tells a more compelling story. In an example of such storytelling, CCP Director of the Office of the Central Commission for Foreign Affairs, Yang Jiechi, in March 2021 during the first Sino-US talks opined, "The United States itself does not represent international public opinion, and neither does the Western world. Whether judged by population-scale or the trend of the world, the Western world does not represent the global public opinion" (*Nikkei Asia*, 2021). Rhetoric will play a key role setting policy for the future direction of global cyber

governance, and both Eastern and Western powers will presumably aim to spin compelling narratives to win allies in their bids for policy wins. Diplomacy certainly has a role in shaping and contesting the rules and practices of cyber governance, and contemporary international power struggles are rhetoric driven to some extent. Through the following investigation, this article further proposes that China has adopted the terminology of "multilateral", "democracy", and "sovereignty" in its diplomatic narrative to challenge existing power structures in the cyber domain.

4. Theoretical Foundation: Discourse as Power

Conventional international relations literature often focuses on a nation state's physical assets, namely territory, technology, and population. However, what brings to this article's attention is that this traditional view cannot explain how the technologically advanced West has not successfully leveraged its material resources to maintain its dominance in the discussion of cyber norms, as witnessed by the growing discussion of China's cyber sovereignty in the international arena. Historically speaking, the US was the creator of the Internet, and many of its technology companies still dominate essential functions within cyberspace (Mueller, 2009: 74-75). However, despite the US's advanced technology and abundant resources in the cyber domain, they seem to fail to dictate the future direction of cyberspace in their favour.

Narrative plays an important role to drive the outcome of discussions on cyber governance, and China's discursive practice is to create a social reality or worldview through narrative and inspire audiences to act upon it. This approach reflects Alexander Wendt's argument that theories literally construct the world and regulate our behaviour (Wendt, 1999: 49). Constructivist approaches emphasise the

critical role of discourse in international relations and examine how the prevailing discourse can result in public consensus (Adler, 1997). Likewise, Foucault argues that discourse is a means of constituting knowledge, together with social practices, forms of subjectivity, and power relations (Weedon, 1987: 108). Hence, discourse and narrative can legitimate an ideological construction, and actions are derived and justified through this given structure. According to Chinese international relations scholar, Qin Yaqing, this type of power "determines the action, position, and identity of every unit inside through its meaning system" (Qin, 2018: 271). However, despite China's focus on the use of diplomatic rhetoric in different issue domains (Zhao, 2016), relatively few studies have attempted to consider the effect of nonmaterial factors in cyber competition.

The international establishment of China's cyber sovereignty discourse can be taken as evidence of China's discursive production. Since Xi Jinping took office, he has emphasised the need to establish international "discourse power" (*huayuquan*). In 2013, he specifically spoke to the CCP Politburo standing committee members and emphasised the need to "tell China's story well" (*jianghao Zhongguo gushi*) (Xinhua, 31st December 2013). In his visit to Brazil during the 2014 BRICS summit, he also highlighted China's intention to ally with developing countries to participate in global governance and create more discourse power (Xinhua, 17th July 2014). Chinese scholar Sun Jisheng, the vice president of the China Foreign Affairs University, has vividly described this strategy as "turning China's words into global words" (*ba Zhongguo huayu zhuanwei shijie huayu*) (Sun, 2019: 36). It is a strategy not about "letting China have a say in international affairs" but about "China's embodiment of power through the use of language" (Rolland, 2020: 10). This study focuses on understanding how the process of

discursive practice has resulted in a new cyber norm for cyberspace and what the implications could be.

5. The Discursive Origin of Cyber Norms

In retrospect, the development of cyber governance has been marked by competing narratives. In 1966, one of the famous Internet pioneers, John Perry Barlow, claimed that "governments of the industrial world … have no sovereignty to cyberspace" (Barlow, 1996). This idea is also reflected in the US's establishment of the earliest cyber governance organization, the Internet Corporation for Assigned Names and Numbers (ICANN), which is a decentralised entity in charge of technical matters and nonjudicial issues. However, with the integration of ICT into the daily life of many, along with the rise of cybercrime and cyberattacks, the international community has quickly discovered the need to regulate activities in cyberspace. The Budapest Convention in 2001 was an early attempt by the European Union to "harmonize" domestic laws across territories to establish a common standard for law enforcement, and it was later ratified by 64 UN member states (Council of Europe, 2021). However, because of a controversial article authorising cross-border investigations (Article 32b), the convention has not been accepted by China and Russia. In addition, the UN hosted the World Summit on Information Security in 2003 and later established the Internet Governance Forum in 2005 to promote discussions regarding global cyber governance. Furthermore, after the massive cyberattacks on Estonia in 2007, the NATO Cooperative Cyber Defence Centre of Excellence initiated a project to prepare the Tallinn Manual on the International Law Applicable to Cyber Warfare, commonly known as Tallinn 1.0, but its revised version from 2017, Tallinn 2.0, has thus far remained purely academic research.

International entities have also been considering the future direction of cyber behaviours, with the West's idea of multi-stakeholder governance looming large in such considerations, but many state and nonstate actors have also proposed initiatives to create common cyber norms. For example, in 2017, Microsoft unsuccessfully proposed the Digital Geneva Convention to ensure private infrastructure could not be exploited by state actors (Jeutner, 2019). France put forth the Paris Call for Trust and Security in Cyberspace without receiving endorsements from China or Russia (Ministry for Europe and Foreign Affairs, France, 2021). Since 2018, the Global Commission on the Stability of Cyberspace has endeavoured to establish general guidelines for states in regard to responsible cyber behaviour but has not achieved a clear consensus.

In short, this review illustrates that the development of cyber norms is still in a volatile stage and achieving a shared understanding of cyber norms is poised to be a contested process that is subject to the influence of myriad discourses by international actors (Niemann and Schillinger, 2017). Nevertheless, given that discourse has keen power to reshape worldviews and influence the global order, whether discourse can be leveraged by China to dominate future discourse is a key question, which is in need of careful investigation and answer in this article.

6. Xi Jinping's Determination to Shape Cyber Norms

China's official statements have repeatedly displayed its strategic intent to increase its leverage in the international discursive space. In 2014, China released a document titled Directives Regarding the Total Fulfilment of Rule by Laws, which specified the need to increase its discourse power and influence (Xinhua, 28th October 2014).

Later that year, the Cyberspace Administration of China was established to coordinate the country's overall policy development and international strategy regarding cyberspace (Central Government, PRC, 27th February 2014). In 2015, Xi called for the international community to follow the principle of state sovereignty enshrined within the UN Charter in efforts to regulate behaviours in cyberspace in his opening remarks at the 2nd World Internet Conference in Wuzhen, China (Xinhua, 16th December 2015). State sovereignty was further elaborated in the CCP's 13th Five-Year Plan, which stated the goals of "the establishment of multilateral, democratic, and transparent international internet governance systems, and [taking] an active part in international cooperation on the formulation of international rules relating to cyberspace security" (National People's Congress, 2016). In 2016, China released its National Cyberspace Security Strategy, in which it restated its ambition to "award its deserved international status" (*guoji diwei xiangcheng*) by establishing its leadership in governance and technological capabilities (CAC, 27th December 2016). In 2017, China's International Strategy of Cooperation on Cyberspace also called for nation states to build "[an] orderly cyberspace and a multilateral, democratic and transparent global Internet governance system" (Ministry of Foreign Affairs, China, 2017). In the first Belt and Road Forum for International Cooperation in 2017, Xi announced the Digital Silk Road and pledged to increase China's influence in cyberspace with further international cooperation (Shen, 2018). As indicated in this context, China has clear strategic intention and sufficient resources, and the next section will investigate how China exercises its discourse power in the international arena.

7. The Discursive Practice of Reshaping International Cyber Governance

Chinese domestic and diplomatic announcements already contain numerous references of cyber sovereignty. In particular, Xi Jinping elaborated on the concept in China's 2nd World Internet Conference in 2015, stating that

> "the principle of sovereignty ***equality*** enshrined in the Charter of the United Nations is one of the basic norms in contemporary international relations … We shall ***respect*** the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and internet public policies, and participate in international cyberspace governance on an equal footing." [emphasis added]
>
> (Xinhua, 16th December 2015)

China's International Strategy of Cooperation in Cyberspace in 2017 also stated, "China supports formulating universally accepted international rules and norms of state behavior in cyberspace with the framework of the United Nations … Relevant efforts should reflect broad participation, sound management[,] and democratic decision making …" (Ministry of Foreign Affairs, China, 2017)

China's strategic narrative has been very evident on various occasions. The earliest apparent effort was in 2011, when the Shanghai Cooperation Organisation (SCO), an regional organization led by China, initiated a motion in the UN called the International Code of Conduct for Information Security; the proposal reaffirmed that "policy authority for Internet-related public issues is the ***sovereign right*** of States" [emphasis added] and "all the rights and responsibilities of States to protect … their information space" (UN General Assembly, 2011). In 2012, China

further proposed modifying the International Telecommunication Regulations to enforce a government-controlled Internet; the suggested amendment did not espouse multistakeholder governance. Although the proposal was not well-received internationally at the time, the concept drew substantial attention (McCarthy, 2011).

Since 2010, amid concerns about states' exploitation of cyberspace, the UN has convened the Group of Government Experts (UNGGE), in which emerging cyber norms have been discussed by the international community (UN General Assembly, 2010). However, in 2015, the SCO submitted an updated version of the International Code of Conduct for Information Security and quoted the UNGGE 2013 report: "State ***sovereignty*** and the international norms and principles that flow from it apply to States' conduct of ICTs-related activities" [emphasis added] (UN General Assembly, 2015b). The SCO's proposal further stated that the state actors shall promote "the establishment of ***multilateral***, ***transparent*** and ***democratic*** international Internet governance" [emphasis added] to ensure equal access to the international discussion of cyber norms. China's strategic intention regarding states' sovereignty has been repackaged using the lexicon of "multilateral", "democracy", and "transparency". This communication strategy has given China the diplomatic high ground to establish much-needed support based on the legacy of the Treaty of Westphalia (Meyer, 2015). However, this does not mean that China agrees with the UNGGE's conclusion entirely. A close examination of the UNGGE discussions reveals that, in 2010, the UNGGE actually agreed with China, but on the additional need to involve nonstate actors in the dialogue, stating in its consensus report that "Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective" (UN General Assembly, 2010). Furthermore, in 2013, the UNGGE seemed to

suggest that states should play important roles in the effort to reduce ICT risks and increase global security, but "effective cooperation would benefit from the appropriate participation of the private sector and civil society" (UN General Assembly, 2013). Instead of borrowing directly from the existing norms in the conventional domains, the 2013 UNGGE report also clearly stated that "Given the unique attributes of ICTs, the report notes that additional norms could be developed over time". However, China's cherry-picking from UN discussions reflects its strategic calculation to shape cyber norms by emphasising the need for state involvement but downplaying the role of the private sector. As part of this ongoing dispute, in 2015, the UNGGE was mandated to discuss the extent to which the existing norms would be applicable in cyberspace (Osula and Roigas, 2016: 119).

China's pick-and-choose approach was more obvious in the 2015 UNGGE discussion. The 2015 UNGGE report stated that "Existing obligations under international law are applicable to State use of ICTs" (UN General Assembly, 2015a). Although China believes that Westphalian sovereignty is applicable in cyberspace, the country disagreed with directly borrowing the existing laws on armed conflicts for the cyber domain (Segal, 2017: 7). China worries that military and civilian infrastructure are difficult to differentiate in cyberspace (Huang and Ying, 2019). The US and China have disputed the origins of various cyberattacks since the US FBI's indictment of five People's Liberation Army hackers in 2014 (Nakashima, 2014), and China worries that accepting the legacy norms of armed conflict in cyberspace presents concerns about escalation amid Sino–US disputes on numerous cyber-incidents (Huang, 2015). The disagreement between the West and China regarding the future of cyber norms runs deep, and no consensus report was drafted pursuant to the 2017 UNGGE discussion (Korzak, 2017).

China eventually established a new UN working group with Russia in 2019 known as the OEWG (UN General Assembly, 2019b). A well-known Chinese cybersecurity expert, Huang Zhixiong, believes that the OEWG is ***open*** (*kaifang*), ***inclusive*** (*baorong*), and ***transparent*** (*touming*) and is open to all UN members to participate in the discussion, which is distinct from the UNGGE's past conduct of secret meetings and closed dialogue (Huang and Liu, 2020). In tandem with this continuous effort to reshape the cyber world, on the 5th November 2019, the UN passed a resolution entitled Countering the Use of Information and Communications Technologies for Criminal Purposes with the backing of China and Russia. The resolution was designed to create a draft working group exclusively for states' participation in the creation of "a new cybercrime treaty" without consulting nonstate actors (UN General Assembly, 2019a). The controversy over enforcing authoritarian states' political online censorship led to 36 human right groups voicing complaints against the resolution, citing its potential to "give wide-ranging power to governments to block websites deemed critical of the authorities, or even entire networks, applications and services that facilitate online exchange of and access to information" (Association for Progressive Communications, 2021).

Thus far, this investigation has indicated that what has contributed to China's initial influence in shaping cyber norms in the UN has relied on the exercise of words, namely power of discourse, instead of material resources or military alliance. The analysis has also highlighted how the lexicon of "democracy", "sovereignty", and "multilateral", terms originating in the West, have been usurped by China and become a "weapon of the weak" to create a counter-hegemonic discourse (Lee, 2012, 85). In the end, China's exercise of discourse power, as orchestrated by Xi Jinping and many Chinese scholars, has entailed it challenging and resisting the existing cyber order defined by the West.

8. Fragmenting Cyberspace and Security Implications

China seeks a leadership position in global cyber governance, and its initial achievement in establishing its own voice can be seen as a product of Xi Jinping's strategy of "improv[ing] our capacity for engaging in international communication so as to tell China's stories well" (Xi Jinping, 2017). Although influencing the discourse of cyber sovereignty represents China's initial success in diluting Western domination of the discussion of cyber norms, it also entails the following implications.

First, China's conceptualization of cyber sovereignty ignores the fact that modern concept of state sovereignty, based on the Treaty of Westphalia, is actually a human invention that is subject to new interpretations. As evidenced by the discussion of the Responsibility to Protect (Badescu, 2011), which argues that the notion that state sovereignty should not just be the protection from outside interference but is a matter of state actors having responsibilities for population's welfare, state sovereignty is conditional and infringeable under specific situations. This comparison indicates that China's state-centric worldview regarding cyberspace may be regarded as anachronistic due to adherence to a definition from 1648. If the conventional concept of sovereignty is already arguable in physical domains, this raises the question of whether the legacy of sovereignty is still appropriate for a brand-new domain created in the late 20th century. This is also to highlight that, when some may interpret China's strategy for cyberspace as grounded primarily in the enhancement of technology and the growth of material resources, this investigation suggests that the competition is also discursive and ideological.

Second, at the international level, were China's narrative of cyber sovereignty to be adopted, the result could be a world with fragmented parts of cyberspace, with each regulated under different domestic laws.

In May 2021, the OEWG released its first consensus report, but so far, it has reaffirmed the agreement achieved in the 2015 UNGGE without delivering any meaningful new achievements (UN General Assembly, 2021). This situation may be due to the international attention primarily occupied by COVID-19, and none of the agreements are ground-breaking, and they may represent the beginning of a slow process of long-term diplomacy (Gold, 2021). However, if China's efforts to rewrite the cyber order prove successful in the future, new cyber norms would partition cyberspace and fundamentally contradict the international community's past efforts, such as the Budapest Convention, to promote agreeable cyber behaviour by harmonizing cyber laws across borders. This assertion of unique territorial jurisdiction may also hinder the advancement of economic activity in cyberspace, as suggested by private enterprises, due to "inconsistent or conflicting national laws and regulations" (Mueller, Mathiason and Klein, 2007: 238-239).

Finally, such a development would also suggest that as China's diplomats and scholars continue to promote cyber sovereignty in the name of protecting the interests of other countries (Cai, 2018: 67; Li, 2019: 109-114), the gradually accepted norm of data localisation or data sovereignty (Streinz, 2021), namely storing domestic data on devices that are physically present within the borders of a country, would allow China to continuously tighten its control over its domestic cyberspace. From this view, championing cyber sovereignty may be aimed at securing China's self-interest in terms of defending its domestic legitimacy.

9. Conclusion

China seeks to reshape cyberspace in a manner that reflects its values and interests, with its efforts depending on discourse power rather than material power. Hence, this article offers an alternative explanation to the conventional focus on technological advancement in the ICT domain. This investigation focuses not on how China's robust tech sector could be a formidable force impacting the international system but rather on how China uses discourse power in its strategic attempt to counter Western dominance. As illustrated by the saying, "Whoever rules the words rules the world" (Rolland, 2020: 7), China's narrative of cyber sovereignty represents utterances with conscious strategic resolve and is not benign communicative discourse. China intends to impose "its preference" through nonviolent means instead of arriving at a consensus with the international community. This analysis also suggests that the international community needs to take a more prudent stance in approaching any claimed knowledge. Language can drive social change in human society, and thus, individuals must be aware of the danger of submitting to unexamined rhetoric without exercising critical reflection.

In summary, cyberspace is a world of human making (Yau, 2018). When the Internet was created, unprecedented connectivity was believed to be a positive development in human society, and it has increased shared understanding and promoted innovation. Nonetheless, many individuals and states no longer believe that cyberspace is a global common that is not subject to state manipulations. Without being overly pessimistic, this trajectory suggests that the future of cyberspace inevitably rests on social agency and individuals' capacity to act independently and make more informed choices.

Notes

+ The early version of this paper was presented at the Conference on "Megatrends in Asia" organized by the Oriental Business and Innovation Center (OBIC), Budapest Business School – University of Applied Sciences, Hungary, in 2021.

* Hon-min Yau (姚宏旻), Ph.D., is an Assistant Professor at the Graduate Institute of Strategic Studies (GISS), National Defense University (國防大學), Taiwan. He received his Ph.D. from the Department of International Politics, Aberystwyth University, Wales, United Kingdom. He was awarded the Michael McGwire Prize by the Department of International Politics in 2016. He also holds a Master of Science in management and information system from Cranfield University, UK. Hence, his research interests are located at the junction of international relations theory, ICT technology, cyber security and national security policy. He contributes to *Issues & Studies*, *Journal of Cyber Policy*, *International Journal of Taiwan Studies*, and *The Korean Journal of Defense Analysis*. <*Email: cf22517855@gmail.com*>

References

Adler, Emanuel (1997). Seizing the middle ground: Constructivism in world politics. *European Journal of International Relations*, Vol. 3, No. 3, Pp. 319-363.

Arquilla, John and David Ronfeldt (eds.) (1997). *In Athena's camp: Preparing for conflict in the information age*. Santa Monica, Ca: Rand Corporation.

Association for Progressive Communications (2021). Open letter To UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online. <*https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human*>

Badescu, Cristina Gabriela (2011). *Humanitarian intervention and the responsibility to protect: Security and human rights*. New York: Routledge.

Barlow, John Perry (1996). A Declaration Of The Independence Of Cyberspace. (San Francisco, CA: Electronic Frontier Foundation.) <*https://www.eff.org/cyberspace-independence*>

CAC (Office of the Central Cyberspace Affairs Commission of the Communist Party of China /中共中央网络安全和信息化委员会办公室) (27th December 2016).《国家网络空间安全战略》全文 [full text of the National Cyberspace Security Strategy]. <*http://www.cac.gov.cn/2016-12/27/c_1120195926.htm*>

Cai Cuihong (2018). Global cyber governance: China's contribution and approach. *China Quarterly of International Strategic Studies*, Vol. 4, No. 1, Pp. 55-76.

Central People's Government of the People's Republic of China (27th February 2014). 中央网络安全和信息化领导小组第一次会议召开 [(Xi Jinping's talk at) the first meeting of the Central Leading Group for Cybersecurity and Informatization]. <*http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm*>

China Daily USA (17th July 2014). Xi: Respect cyber sovereignty. <*http://usa.chinadaily.com.cn/epaper/2014-07/17/content_17818027.htm*>

Council of Europe (23rd April 2021). Chart of signatures and ratifications of Treaty 185. <*https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185*>

Financial Times (23rd April 2021). China's central bank fights Jack Ma's Ant Group over control of data. <*https://www.ft.com/content/1dbc6256-c8cd-48c1-9a0f-bb83a578a42e*>

Gold, Josh (2021). Unexpectedly, all UN countries agreed on a cybersecurity report. So what? *Blog Post*, 18th March 2021. New York: Council on Foreign Relations. <*https://www.cfr.org/blog/unexpectedly-all-un-countri*

es-agreed-cybersecurity-report-so-what>

Huang Zhixiong (黄志雄) (2015). 国际法视角下的“网络战”及中国的对策——以诉诸武力权为中心 [International legal issues concerning “cyber warfare” and strategies for China: Focusing on the field of jus ad bellum]. *Modern Law Science*, 5, pp. 145-158.

Huang Zhixiong and Liu Xinxin (黄志雄、刘欣欣) (2020).2020年上半年联合国信息安全工作组进程网络空间国际规则博弈 [the competition of international rules on cyberspace in the process of the United Nations OEWG in the first half of 2020]. *China Information Security*, 7, pp. 68-71.

Huang Zhixiong and Ying Yaohui (黄志雄、应瑶慧) (2019). 论区分原则在网络武装冲突中的适用——兼评《塔林手册 2.》相关内容 [on the application of the principle of distinction in the cyber armed conflict——via the perspective of Tallin 2.0”]. *Journal Of Yunnan Minzu University*, 36(5), pp. 135-149.

Internet Live Stats (2016). Internet users by country (2016). *<https://www.internetlivestats.com/internet-users-by-country/>*

Jeutner, Valentin (2019). The digital Geneva Convention: A critical appraisal of Microsoft’s proposal. *Journal Of International Humanitarian Legal Studies*, Vol. 10, No. 1, pp. 158-170.

Korzak, Elaine (2017). UN GGE on cybersecurity: The end of an era? *The Diplomat*, 31st July 2017 (The Debate).

Lee, Donna (2012). Global trade governance and the challenges of African Activism in the Doha Development Agenda negotiations. *Global Society*, Vol. 26, No. 1, pp. 83-101.

Li Yan (2019). Global cyberspace governance: State actors and the China-US cyber relationship. *Contemporary International Relations*, Vol. 29, No. 2, pp. 105-124.

Lu Wei (2014). Cyber sovereignty must rule global Internet. *Huffpost* (*The Huffington Post*), 15th December 2014. *<http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html>*

McCarthy, Daniel R. (2011). Open networks and the open door: American foreign policy and the narration of the Internet. *Foreign Policy Analysis*, Vol. 7, No. 1, pp. 89-111.

Meyer, Paul (2015). Seizing the diplomatic initiative to control cyber conflict. *The Washington Quarterly*, Vol. 38, No. 2, pp. 47-61.

Ministry for Europe and Foreign Affairs, France (2021). Paris Call for Trust and Security in Cyberspace. <*https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace*>

Ministry of Foreign Affairs, China (1st March 2017). 网络空间国际合作战略 [international strategy of cooperation on cyberspace]. <*https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t1442389.shtml*>

Mueller, Milton, John Mathiason and Hans Klein (2007). The Internet and global governance: Principles and norms for a new regime. *Global Governance: A Review of Multilateralism and International Organizations*, Vol. 13, No. 2, pp. 237-254.

Mueller, Milton L. (2009). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge , MA: MIT Press.

Nakashima, Ellen (2014). Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyberspying. *The Washington Post*, 22nd May 2014. <*https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html*>

National People's Congress of the People's Republic of China (2016). *13th Five-Year Plan for Economic and Social Development of the People's Republic of China (2016-2020)*. Beijing: Central Compilation & Translation Press.

Niemann, Holger and Henrik Schillinger (2017). Contestation 'all the way down'? The grammar of contestation in norm research. *Review of*

International Studies, Vol. 43, No. 1, pp. 29-49.

Nikkei Asia (19th March 2021). How It happened: Transcript of the US-China opening remarks in Alaska. <*https://asia.nikkei.com/Politics/International-relations/US-China-tensions/How-it-happened-Transcript-of-the-US-China-opening-remarks-in-Alaska*>

Osula, Anna-Maria and Henry Rõigas (eds.) (2016). *International cyber norms: Legal, policy & industry perspectives*. Tallinn: The Nato Cooperative Cyber Defence Centre of Excellence.

Qin, Yaqing (2018). *A relational theory of world politics*. Cambridge: Cambridge University Press.

Qiu, Jack Linchuan (2003). The Internet in China: Data and issues. (Working paper prepared for Annenberg Research Seminar on International Communication, October 1, 2003).

Rolland, Nadège (2020). *China's vision for a new world order.* Seattle, Wa: National Bureau of Asian Research (NBR).

Segal, Adam (2017). Chinese cyber diplomacy in a new era of uncertainty. *Aegis Paper Series* No. 1703. Washington, D.C.: Hoover Institution.

Shen, Hong (2018). Building a digital Silk Road? Situating the Internet in China's Belt And Road Initiative. *International Journal Of Communication*, Vol. 12, pp. 2683-2701.

Streinz, Thomas (2021). RCEP's contribution to global data governance. *Afronomicslaw*, 19th February 2021. <*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826217*>

Sun Jisheng (孙吉胜) (2019). 中国国际话语权的塑造与提升路径 [approaches of constructing and elevating China's discourse power]. *World Economics and Politics*, 3.

Taiwan News (6th July 2021). China uses Didi as data law test dummy. (Reported by Reuters.) <*https://www.taiwannews.com.tw/en/news/4241463*>

United Nations (2019). China's submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. <*https://www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf*>

UN General Assembly (2010). Group Of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201). <*https://undocs.org/zh/a/65/201*>

UN General Assembly (2011). Letter dated 12 september 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359). <*https://www.un.org/zh/documents/view_doc.asp?symbol=a/66/359*>

UN General Assembly (2013). Group Of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98). <*https://undocs.org/zh/a/68/98*>

UN General Assembly (2015a). Group Of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). <*https://undocs.org/zh/a/70/174*>

UN General Assembly (2015b). Letter dated 9 january 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/69/723). <*https://undocs.org/zh/a/69/723*>

UN General Assembly (2019a). Countering the use of information and communications technologies for criminal purposes (A/C.3/74/L.11/Rev.1). <*https://undocs.org/en/a/c.3/74/l.11/rev.1*>

UN General Assembly (2019b). Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of

International Security (A/AC.290/2019/1). <*https://undocs.org/zh/a/ac.290/2019/1*>

UN General Assembly (2021). Open-ended Working Group on Developments In the Field of Information and Telecommunications in the Context of International Security – Final Substantive Report (A/AC.290/2021/CRP.2). <*https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf*>

Weedon, Chris (1987). *Feminist practice and poststructuralist theory.* Oxford and New York: B. Blackwell.

Wendt, Alexander (1999). *Social theory of international politics*. Cambridge: Cambridge University Press.

Xi Jinping (习近平) (18th October 2017). 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 a new era. (Delivered at the 19th National Congress of the Communist Party of China, October 18, 2017). <*http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf*>

Xinhua News Agency (31st December 2013). 習近平：建設社會主義文化強國　著力提高國家文化軟實力 [Xi Jinping: establish a strong socialist-culture country, and enhance national soft power]. Beijing: Central People's Government of the People's Republic of China. <*http://big5.www.gov.cn/gate/big5/www.gov.cn/ldhd/2013-12/31/content_2558147.htm*>

Xinhua News Agency (17th July 2014). 习近平在巴西国会的演讲 [Xi Jinping's speech at the National Congress of Brazil (Brasilia, July 16, 2014)]. *Xinhuanet*. <*http://www.xinhuanet.com//world/2014-07/17/c_1111665403.htm*>

Xinhua News Agency (28th October 2014). 中共中央关于全面推进依法治国若干重大问题的决定 [CPC's directives regarding the total fulfillments of rule by laws]. Beijing: Central People's Government of the People's

Republic of China. <*http://www.gov.cn/xinwen/2014-10/28/content_2771714.htm*>

Xinhua News Agency (16th December 2015). 习近平在第二届世界互联网大会开幕式上的讲话（全文）[Xi Jinping attended the opening ceremony of the Second World Internet Conference and delivered a keynote speech (full text)]. *Xinhuanet*. <*http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm*>

Yau, Hon-min (2018). Explaining Taiwan's cybersecurity policy prior to 2016: Effects of norms and identities. *Issues & Studies*, Vol. 54, No. 2, Article 1850004. doi:10.1142/S1013251118500042

Yau, Hon-min (2019). An assessment of cyberpower within the triangular relations of Taiwan–Us–China and its implications. *International Journal Of Taiwan Studies*, Vol. 2, No. 2, pp. 264-291.

Zhao, Kejin (2016). China's rise and its discursive power strategy. *Chinese Political Science Review*, Vol. 1, No. 3, pp. 539-564.