The International Spectator
Italian Journal of International Affairs

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rspe20

An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model

Xinchuchu Gao

To cite this article: Xinchuchu Gao (2022): An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model, The International Spectator, DOI: 10.1080/03932729.2022.2074710

To link to this article: https://doi.org/10.1080/03932729.2022.2074710

Published online: 27 May 2022.

THE INTERNATIONAL SPECTATOR
https://doi.org/10.1080/03932729.2022.2074710

RESEARCH ARTICLE

OPEN ACCESS

An Attractive Alternative? China’s Approach to Cyber Governance and Its Implications for the Western Model

Xinchuchu Gao

European Institute, London School of Economics and Political Science

ABSTRACT

China’s cyber norm-building efforts can be usefully explored based on the concept of the norm life cycle developed by Finnemore and Sikkink. Although China puts cyber sovereignty and government involvement at the core of its cyber governance approach, its Internet policies are a result of interactions between state agencies and business units, and recent reforms suggest greater involvement of Chinese companies. Moreover, many countries, including some from the West, have placed increasing emphasis on intergovernmental involvement and data sovereignty when developing their Internet policies. The EU, for instance, believes that digital sovereignty is necessary to protect its own market from US and Chinese technology giants. Despite the fundamental differences between Brussels’s digital sovereignty and Beijing’s cyber sovereignty, the dichotomy between China’s sovereignty-oriented approach and the more open approach of Western countries is more blurred than it may appear, leading to Western countries, the EU in particular, potentially becoming more receptive to China’s cyber norms.

KEYWORDS

cyber governance; cyber sovereignty; EU; China

Global cyber governance has long been dominated by the United States (US). However, the shifting geopolitics of cyberspace in the post-Snowden era and the rise of new cyber powers have challenged the US hegemonic position both inside and outside the Western bloc. Competition in cyberspace has escalated to the extent that the situation is now termed the “Digital Cold War” (Crovitz 2012; Reddy and Soni 2021).

China, a leader among emerging cyber powers, has turned into a strong competitor. Having the world’s largest online population of 898 million (CNNIC 2021) and a prosperous information and communications technology (ICT) sector, Beijing has become a key player in global cyberspace. The People’s Republic of China (PRC) has indeed made significant efforts to set cyber norms (Segal 2020), which have positioned it to become a norm- and regulation-setter in cyberspace.

Discussion of China’s cyber governance approach has primarily focused on the notion of ‘cyber sovereignty’, which supposedly allows all countries to cooperate in cyberspace on the basis of equality, as well as the Chinese government’s involvement in controlling

CONTACT Xinchuchu Gao ✉ x.gao5@lse.ac.uk @chuchu62943666

the digital sphere. Confrontation between Washington and Beijing in cyberspace therefore may be cast as an open multi-stakeholder approach vs. a sovereignty-driven and government-dominated approach. This dichotomy is often described in terms of a West vs. non-West confrontation (Liu 2012).

Although this dichotomy offers important insights into both the global landscape of cyber governance and China's cyber governance approach, it oversimplifies the PRC's position and overlooks shifts in global cyber governance. On the one hand, the conventional cyber sovereignty understanding of China's approach reduces it to sovereignty concerns and government interventionism. However, recent scholarship acknowledges greater complexity in Beijing's position. For example, by analysing Global South countries' Internet-related negotiations at the World Summit on the Information Society, Abu Bhuiyan (2014) observed ambiguity in China's position and pointed out that the PRC chose to acquiesce to the US in some cases. Although China called for more equitable Internet governance, it did not question the neoliberal basis of the existing governance scheme (Ibid.). In a similar vein, after analysing the friction between China and the global cyber governance approach over the last three decades, Hong Shen (2016, 320) noted that the "cyber sovereignty" framework failed to capture and interpret the PRC's cyber governance approach. China's policy formation can be read as the product of complex interactions among different state agencies and business units. Shen argued that China's cyber governance approach has been influenced by competing interests among domestic businesses as well as interaction among businesses in both domestic and transnational contexts (Ibid.)

On the other hand, the West vs. non-West approaches to cyber governance are seen as two homogenous blocs, overlooking the increasing divergence of opinion within the Western bloc. In particular, the EU's emergence as a distinctive cyber power has challenged the US as a hegemon in cyberspace. Despite sharing core cyber values and norms with Washington, Brussels promotes its own approach to cyber governance (Dunn Cavelty 2018).

In line with the objective of this Special Core, this article aims to overcome the West vs. non-West dichotomy in global cyber governance. First, by analysing the principal norms guiding China's cyber practices and unpacking the interaction between government and business, it seeks to move beyond the conventional cyber sovereignty framework to understand China's cyber governance approach. Second, by examining the extent to which Beijing has been successful as a norm entrepreneur, it investigates different levels of receptiveness to China's cyber norms, including among Western bloc countries. The following research questions are addressed: What are the principal norms driving China's cyber governance approach? How has the PRC attempted to establish its cyber norms? To what extent has it been successful as a norm entrepreneur?

The article is structured as follows. The first section provides background on the landscape of global digital governance, examining in particular the growing divergence in attitudes to cyber governance in the US and the EU. The second section draws on the literature on norm entrepreneurship to provide an analytical framework. The third section uses this framework to examine China's norm-building attempts in the field of digital governance. The article concludes with an evaluation of how successful China has been thus far and implications for global cyber governance.

Setting the scene: the evolving landscape of global cyber governance

Global cyber governance is arguably dominated by a Western-centric approach, which is characterised by commitment to multi-stakeholderism and fundamental values, including the free flow of information, human rights and democracy (DeNardis 2014). The US has held a leadership role in promoting this approach. However, an increasingly complex global geopolitical environment has created obstacles to the Western-centric approach. As Xuechen Chen and Yifan Yang (2022, forthcoming) argue, the increasing influence of the EU as a distinctive cyber power has called into question the US dominance in cyberspace within the Western bloc. Additionally, the approaches adopted by emerging non-Western cyber powers, such as China and Russia, have further contributed to undermining the Western-centric cyber governance approach, promoting a multilateral approach that prioritises the role of sovereign states in governing cyberspace (Liaropoulos 2016).

The Western-centric approach to cyber governance and differentiation within it

Western countries share a number of cyber values and norms, such as multi-stakeholderism, "a constantly shifting balance of powers between private industry, international technical governance institutions, governments and civil society" (DeNardis 2014, 226–7). In this vision, cyber governance takes place in a multi-stakeholder structure based on "openness, inclusion, bottom-up collaboration and consensual decision-making" (Pohle and Thiel 2020, 5). This form of coordination could counteract the need for the involvement of sovereign states (Raymond and DeNardis 2015).

Another common principle shared by Western countries is that global cyber governance should protect fundamental rights, particularly freedom of expression and the free flow of information (Anagnostakis 2021). For example, one of the priorities of the US–EU Cyber Dialogue is close coordination of EU and US policy on the promotion of human rights online in international fora such as the "Freedom Online Coalition" (White House 2014). Similarly, the G7 established the Roadmap for Cooperation on Data Free Flow with Trust at the G7 Digital and Technology Ministers' meeting in April 2021. This roadmap was endorsed by two guest countries, South Korea and Australia (G7 2021).

Nevertheless, the Western-centric approach to cyber governance has been undermined by increasing divergence within the Western bloc. In particular, the EU has challenged the US leadership role. As mentioned, the EU and the US share core values and norms relating to cyber governance in that they both endorse principles such as openness, freedom and multi-stakeholderism, but Brussels's approach differs from Washington's in terms of the level of government involvement. The US approach has been described as "hands-off-the-Internet", that is, limited governmental involvement. The EU, instead, has historically been more willing to embrace cyber regulation than the US (Taylor and Hoffmann 2019). The EU finds it conceptually troubling that government authorities play a less important decision-making role than private corporations (O'Hara and Hall 2018). George Christou (2014) points out that the EU has increasingly emphasised the importance of government involvement in cyberspace. For example, the EU supports a greater role for the Governmental Advisory Committee and the inclusion of sovereign states such as India and Brazil in the Internet Corporation for Assigned Names and Numbers (ICANN) (Taylor and Hoffmann 2019).

Moreover, the EU is increasingly promoting the concepts of "technical sovereignty", "digital sovereignty" and "data sovereignty" (Scott 2019). Brussels's willingness to pursue sovereignty in cyberspace is principally driven by concerns over falling behind the US and China in the global information technology market. The Digital Economy Report (UNCTAD 2019) shows that China and the US account for 75 per cent of all patents related to blockchain technologies and over 75 per cent of the global public cloud computing market. To Brussels, relying on non-EU technology companies threatens EU citizens' control of their data, thus undermining Europe's leadership and strategic autonomy in cyberspace. The EU is therefore increasingly striving for sovereignty in cyberspace. As French President Emmanuel Macron (2020) stated, "European freedom of action requires economic and digital sovereignty". Similarly, in July 2020, the German Presidency of the Council of the EU, in its manifesto, announced the EU's intention "to establish digital sovereignty as a leitmotiv of European digital policy" (European Parliament 2020a). In 2020, the European Parliament issued the report "Digital Sovereignty for Europe", which defines digital sovereignty as "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)" (European Parliament 2020b). In conclusion, the EU's promotion of sovereignty in cyberspace is mostly a result of security concerns over dependence on non-EU technology companies and the desire to play a leadership role in digital innovation.

Alternative digital governance approaches promoted by emerging cyber powers

The Western-centric cyber governance approach has been challenged by a group of countries outside the Western bloc, including emerging countries such as China, Russia, Brazil and South Africa (Rebello 2017). These countries argue that the existing global cyber governance framework puts newcomers at a disadvantage. For example, a number of countries have refused to ratify the Council of Europe Convention on Cybercrime, also known as the Budapest Convention, either because they did not participate in the drafting process or because the Convention disregards their claims of state sovereignty in cyberspace (Hakmeh 2017).

These countries also challenge US leadership in cyber governance. As Shen (2016) states, Edward Snowden's revelations contributed to questioning the legitimacy of the US-dominated cyber governance framework. A number of developing countries have subsequently questioned US hegemony in cyber governance. They argue that the Snowden leaks prove that the US exploits mass surveillance data without any oversight, highlighting Washington's hypocritical behaviour in cyberspace (Farrell and Finnemore 2013).

To sum up, the Internet's continuing expansion has led to increased competition in cyberspace and its governance. US hegemony in the field of cyber governance has been challenged from both within and without the Western bloc.

Norms and norm entrepreneurship in cyberspace

An international norm can be conceptualised as a “set of standards for the appropriate behavior of states” (Finnemore and Sikkink 1998, 893). An international norm can be understood as an international policy fashion, defining what behaviour is considered appropriate and what is not. Effective cyberspace governance requires universally accepted norms, but these norms remain highly contested (Broeders and van der Berg 2020, 5).

Martha Finnemore and Kathryn Sikkink (1998) argue that norms are often promoted by a norm entrepreneur. They detail a three-stage process, which creates a “norm life cycle”. The first stage is norm emergence; the second is broad norm acceptance; and the last is internationalisation. In the first stage, where norms are shaped, the role of norm entrepreneurs is vital. A norm entrepreneur can be defined as an “agent having strong notions about appropriate or desirable behaviour in their community” (896). They attempt to convince other actors to accept new norms by calling attention to issues, or even creating issues by dramatising them. In this stage, organisational platforms, often in the form of international organisations, are needed for the promotion of norms. In the second stage, a number of actors accept the norms and convince others to accept them, what is termed a ‘norm cascade’ or broad norm acceptance. Finally, the norms gain a taken-for-granted status, which means they have been internationalised.

Finnemore and Sikkink’s concept of the norm life cycle has been used to analyse the emergence of cyber norms with a focus on Western countries’ efforts. Tim Maurer (2011), for example, uses it to calculate how much attention cybersecurity-related issues have received from UN organisations and UN member states, particularly Russia and the US. He concludes that voting patterns, co-sponsorship of draft resolutions and the content and language of resolutions demonstrate the emergence of cyber norms. Matthew Crandall and Collin Allan (2015) use Finnemore and Sikkink’s theoretical framework to analyse whether NATO membership has allowed a small state such as Estonia to be successful in norm-building. They conclude that it has indeed helped but with limitations; despite these limitations, in their view, securing a role as a norm entrepreneur is a powerful way for small states to ensure state interest globally. Similarly, Liisi Adamson and Zine Homburger (2019) examine the potential of small states to become norm entrepreneurs in cyberspace. Focusing on the Netherlands and Estonia, they argue that small states, especially highly developed ICT states, could be natural cyber norm entrepreneurs. As far as the US is concerned, Tim Stevens (2012) looks into its role in forming cyber norms and questions whether such norms are being established. He argues that there has been little progress in cyber deterrence, while pointing out that the US has successfully promoted cyber norms based on its neoliberal worldview. Martha Finnemore and Duncan Hollis (2016) instead explore the *process* of constructing norms for global cybersecurity. They argue that, while “calls for ‘cyber norms’ to secure and govern cyberspace are now ubiquitous”, cybersecurity is actually “a diverse array of problems”. They further point out that the value of cyber norms lies in the process by which they are formed (207).

There have also been several studies of non-state actors’ attempts to construct global cybersecurity norms. Louise Marie Hurel and Luisa Lobato (2018), for instance, use Microsoft as an example to unpack the role of private companies as norm entrepreneurs.

Similarly, Carol Glen (2021) argues that while states remain central, non-state actors are playing an increasingly significant role in forming cyber norms.

Overall, the existing literature on cyber norm-building and the adoption of Finnemore and Sikkink's concept of the norm life cycle has mainly focused on Western countries and private companies. Recently, however, some scholars have examined China's cyber norm-setting attempts. Yu Hong and Thomas Goodnight (2019), for example, argue that China's construction of cyber sovereignty is primarily driven by the desire to safeguard the multipolar global digital order and ensure global wellbeing. Rogier Creemers (2020) examines the development of China's conception of sovereignty and identifies two major components: a normative component, which guides states' behaviour in cyberspace; and a capability component, that is, the governance resources required for a state to realise the normative component. Jinghan Zeng *et al.* (2017) unpack Chinese domestic discourse on the concept of Internet sovereignty and argue that the formulation of the concept has been fragmented, which has significantly restricted China's capacity to promote alternative cyber norms in global cyberspace. Nevertheless, the existing literature does not explicitly study the acceptance of China's cyber norms at the international level. This study, instead, aims to fill the gap by analysing China's role as a norm entrepreneur in cyberspace, applying Finnemore and Sikkink's theoretical framework to Beijing's attempts to establish cyber norms and examining their acceptance.

China as a cyber norm entrepreneur

Building China's cyber norms

China has one of the most active digital ecosystems in the world. It is the world's second-largest digital economy after the US (Meltzer 2020). In 2020, China's digital trade hit USD 203.6 billion, accounting for 26 per cent of Beijing's total trade in services (*Xinhua* 2020). Meanwhile, China has been at the forefront of commercialising digital business models. The past decade has seen the rise of tech giants in China, such as Baidu, Alibaba and Tencent. The global reach of these companies has the potential to reshape the digital ecosystem (Woetzel 2017). Moreover, the outbreak of Covid-19 at the end of 2019 boosted the growth of digital businesses, further contributing to the digital transformation of the Chinese economy (Zipser and Poh 2021).

Using its fast-growing ICT industry, the PRC has implemented a strategy to make it a cyber great power. For instance, China's Deputy Information Technology Minister Chen Zhaoxiong (2019) wrote that China should grab the strategic opportunity to become a cyber great power. In a similar vein, an article by Xu Zhengzhong (2020) in *Party & Government Forum*, a journal run by the Central Party School of the Chinese Communist Party, points out that fifth-generation (5G) technologies offer a chance to strengthen China's global competitiveness.

Indeed, Beijing has made increasing efforts to establish itself as a creator and promoter of cyber norms. At the Second World Internet Conference, President Xi (2015) declared that the construction of "appropriate Internet governance norms" was a vital part of the strategy to make China a cyber great power. Similarly, an article in leading party journal *Qiushi* (2017) stated that strengthening China's influence over global cyberspace was key.

More recently, Xu Zhengzhong (2020) argued that, in the Internet era, developing the discourse and rule-making power in cyberspace was a priority.

As mentioned, a cornerstone of China's normative position on cyberspace is the concept of cyber sovereignty. This concept shapes its domestic policy as well as its international cyber diplomacy, in sharp contrast with the free flow of information that is so vital to the US, the EU and those whose interests align with them. Cyber sovereignty first appeared prominently in China's 2010 White Paper outlining its approach to cyberspace. In this paper, China maintained that all countries should cooperate in cyberspace "on the basis of equality and mutual benefit" (SCIO 2010). Sovereignty also featured as the first of five international cooperation principles in cyber governance proposed by the PRC's delegation at the Budapest Conference on Cyberspace 2012. In this proposal, cyber sovereignty was defined as "policy authority for Internet-related public policy issues" (Huang 2012). At the World Internet Conference in 2015, President Xi (2015) pointed out the risks of not allowing sovereign states to govern their cyberspace according to their own rules and stressed the need to respect their sovereign equality. The most comprehensive description of cyber sovereignty can be found in the "International Strategy of Cooperation on Cyberspace" issued in 2017 by the Ministry of Foreign Affairs of the People's Republic of China. This document stresses that the principle of sovereignty covers all aspects of state-to-state relations, including cyberspace, so "countries should respect each other's right to 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" (Ministry of Foreign Affairs of the People's Republic of China 2017).

Beijing has also stressed the principle of multilateralism in cyber governance. Unlike the private-sector-led multi-stakeholder approach promoted by many Western states, China calls for a multilateral approach to governing cyberspace, with an emphasis on greater government involvement and a leading role for the UN in building an international consensus on rules (Cai 2018). The PRC has been signalling a multilateral approach to governing cyberspace at least since the publication of its White Paper in 2010. This advocated for multilateral cooperation to address "the increasingly serious problem of transnational network crimes". In particular, the document stressed that "the Chinese government plays the leading role in Internet administration" (SCIO 2010). In a 2015 article, Lu Wei, then head of the Cyberspace Administration of China, explained the major difference between a multi-stakeholder and a multilateral approach. According to him, a multi-stakeholder approach follows a "people-centred" logic that allows all Internet participants to make the rules on an equal footing, while a multilateral approach means that the state sets the rules based on the idea of cyber sovereignty (Lu 2015). For China, the private-sector-led multi-stakeholder approach led to the cross-border, private, distributed architecture of the Internet, which poses a threat to state sovereignty (DeNardis 2020). The PRC's multilateral approach to cyber governance is thus primarily driven by sovereignty concerns.

In addition to its desire to protect state sovereignty, China's promotion of a multilateral approach reflects its desire to challenge the US hegemonic position in cyberspace. Beijing maintains that Washington has too much power in the current multi-stakeholder model and calls for the voice of new cyber powers to be heard in international Internet governance institutions such as the ICANN and the Internet Governance Forum (Christou 2014).

Despite Beijing's focus on cyber sovereignty and government involvement in its cyber governance approach, however, as Zhao Yuezhi (2010) points out, China's position on cyber governance is not simply defined by government authorities, but rather a result of interactions between state agencies and businesses.

A telling example of the significant influence of business on China's cyber governance approach is Beijing's failed attempts to mandate a new wireless local area network (LAN) standard, Wireless LAN Authentication and Privacy Infrastructure (WAPI), instead of the widely used Wi-Fi wireless connection standard. China's promotion of WAPI standards was primarily driven by concerns about security deficiencies in Wi-Fi standards (Zhao 2010). Ever since the approval of Wi-Fi in 1999, independent analysts have noted the apparent weakness of Wi-Fi's encryption component, so China was keen to promote its own standard. In 2003, the Standardization Administration of China submitted WAPI to the International Organization for Standardization (ISO) for international recognition. However, the ISO rejected WAPI in 2006 (Clendenin 2006). The Chinese government resubmitted its proposal in 2007 but withdrew it in 2011, so WAPI standards failed to achieve international recognition (Kim *et al.* 2020).

When China tried to push WAPI internationally, it faced challenges from transnational capital, led by Intel Corporation, and foreign governments. In addition to external resistance, the PRC government's ability to get WAPI internationally accepted was constrained by diverging interests between Chinese state agencies and companies (Zhao 2010). The developer and owner of WAPI was a small technology company, Jietong, which meant that well-established companies such as Huawei, Lenovo and ZTE had little interest in supporting it, citing concern about the economic cost of developing China's own version of wireless encryption standards (Kennedy 2006). Although these companies did not hold decision-making positions in the ISO, their reluctance to accept WAPI undermined the Chinese government's agenda-setting power (Shen 2016). The WAPI case implies that China's domestic businesses do not always support their government's views. Therefore, although China's cyber governance approach is primarily driven by its desire to protect state sovereignty and increase government involvement, interactions between state agencies and businesses have had a determining influence in shaping it.

Moreover, although it is unlikely that China's cyber governance approach will be transformed into a fully industry-driven approach in the short term, recent reforms demonstrate the possibility of greater involvement by Chinese businesses. For example, within the limitations of a state-dominated approach to standardisation, the PRC has allowed Chinese companies to play a greater role in developing technical standards. As early as 2014, China initiated a set of reforms aiming to empower organisations outside the government, which has then continued under the banner of China Standards 2035, a programme promoted by the Standardisation Administration of China. In October 2021, China's State Council's (2021) national strategy for technical standards was released. This new strategy does not call for a break with Beijing's state-dominated approach but demands nonetheless a larger role for industry actors (Sheehan *et al.* 2021). This is one of China's many recent reforms in cyberspace;

while cyber sovereignty and government involvement remain central, the influence of business on the development of cyber policies is growing. This increases the possibility of a convergence between China's and Western countries' approaches to cyber governance.

China's attempts at establishing cyber norms

To promote the above-mentioned cyber norms, Beijing has established itself as a norm entrepreneur in cyberspace, thus contributing to norm emergence. Indeed, China has put forward its cyber norms in several state-led multilateral and regional fora in an attempt to reshape global discourse on cyber governance. For example, it has actively used the UN as an organisational platform to participate in the normative debate on cyber governance. Beijing considers the UN "the most legitimate global body" because all countries participate in it (Bhuiyan 2014). In its 2010 White Paper, China argued that "the UN should be given full scope in international Internet administration" (SCIO 2010). At the UN, China has consistently stressed the importance of cyber sovereignty and government involvement in cyber governance. For example, China observed that sovereign governments should act as the leading players under the United Nation's framework (Bull *et al.* 2004). In the UN Group of Governmental Experts (GGE), China and Russia have resisted US efforts to apply the laws of armed conflict and the right of self-defence to cyberspace. Partly due to China and Russia's opposition, GGE-participating countries failed to reach a consensus on a follow-up report on a related US proposal in 2017. In the wake of this failure, Russia proposed creating the UN Open-Ended Working Group (OEWG) on ICTs to discuss the formulation of international norms and rules in cyberspace. China's submissions to the OEWG explicitly reflected its normative position on cyberspace. The Chinese Representative (2019, 2) noted that it was "widely endorsed by the international community that the principle of sovereignty applies in cyberspace".

In addition, China's efforts are bolstered by the Belt and Road Initiative and the Digital Silk Road (DSR). As Clayton Cheney (2019) states, the DSR plays an important role in China's efforts to export its version of cyber governance. In line with the going-out strategy, the PRC's government and high-tech companies aim to export China's digital products and provide ICT infrastructure in participating countries. The DSR also supports the Chinese approach to Internet governance (Ibid.). Although promoting the Chinese version of cyber norms is not part of the official rhetoric on the DSR, there is a general concern among Western states that China is willing and able to export its cyber norms through providing cyber products, technologies and infrastructure (Ghiasy and Krishnamurthy 2020). As Sally Adee (2019) has pointed out, China is offering "a full kit […] to execute a Chinese version of the Internet". In this sense, the DSR goes beyond providing physical infrastructure to export ideological principles regarding cyber governance (Cheney 2019).

When conducting DSR projects, China promotes multilateralism and intergovernmental collaboration. In the report "The Belt and Road Initiative: Progress, Contributions and Prospects", Beijing stressed the importance of establishing a "multilateral, democratic, and transparent international Internet governance system", underlining its preference for multilateralism (Office of the Leading Small Group for Promoting the

Work of Constructing the "Belt and Road Initiative" 2019). China has also signed many agreements with partner countries. Examples include Bilateral Memoranda of Understanding with the governments of Cambodia, Iran, Bangladesh and Afghanistan, as well as an action plan strengthening a partnership for the joint development of ICTs between China and the Association of Southeast Asian Nations (Gong and Li 2019). Moreover, Beijing has firmly established cyber sovereignty as the guiding principle when conducting DSR projects. "Full respect" for cyber sovereignty is explicitly identified as one of the fifteen general principles of the DSR, encouraging the construction of "peaceful, safe, open, cooperative, and orderly cyberspace", and principle 13 encourages "cooperation and respect for independent development" (Office of the Central Cyberspace Affairs Commission 2018). This language is in line with China's general emphasis on respect for sovereignty and independence in cyberspace.

The PRC has also enforced its norm-promoting role in regional organisations. The Shanghai Cooperation Organisation, for instance, is a major forum in which China engages with like-minded countries to shape the debate on norm development in cyberspace. In 2011, China and Russia, along with the other members of the Organisation (Tajikistan, Uzbekistan, Kyrgyzstan and Kazakhstan), jointly submitted the "International Code of Conduct for Information Security" to the UN. This code of conduct, which aimed to shape new norms in cyberspace, was rejected by the US and most Western states, which consider a sovereignty-centred cyber governance approach as a potential tool of oppressive regimes (Zeng *et al.* 2017). Despite its initial failure, an updated version submitted to the UN in 2015 still emphasised Internet sovereignty (Rõigas 2015). Similarly, the 2017 BRICS (China, Brazil, Russia, India and South Africa) Leaders Declaration put particular emphasis on principles of international law enshrined in the Charter of the United Nations, "particularly the state sovereignty" (BRICS Summit 2017).

Acceptance of China's cyber norms

Moving to the second and third stages of the norm life cycle faced by China's cyber norms, Beijing's sovereignty narrative is indeed attractive to a number of emerging cyber powers as well as to small and mid-size cyber players. For instance, following China's proposal of the agenda item "International Law in Cyberspace" at the 53rd Annual Session of the Asian–African Legal Consultative Organisation in 2014, the organisation established a working group to discuss state sovereignty and international cooperation in cyberspace (Huang 2016).

Another indication of acceptance of China's cyber governance approach is the number of countries that have participated in the DSR. By 2019, China had signed cooperative agreements with sixteen countries under the DSR framework (Office of the Leading Small Group for Promoting the Work of Constructing the "Belt and Road Initiative" 2019). To be sure, Western companies such as Sweden's Ericsson and Finland's Nokia are also focusing on emerging markets in developing 5G networks, thus competing with Chinese firms. Nevertheless, both Ericsson and Nokia are losing ground to Huawei and ZTE. Indeed, Huawei has finalised more 5G contracts than any other telecom company: by 2020, it had 91 commercial 5G contracts, while Ericsson 81 and Nokia just 67 (Si 2020).

Developing countries are receptive to China's cyber governance approach for two main reasons. First, some countries outside the Western bloc have long been reluctant to accept the Western-centric approach because their voices are less heard within it. In particular, they see cyber sovereignty as a way to diminish US hegemony in cyberspace. For instance, Zimbabwe, Djibouti and Uganda have concerns over joining an Internet "that's just a gateway" for companies such as Google and Facebook to colonise their digital space; they prefer an Internet based on non-Western standards and values. Internet construction under DSR-related projects therefore appears an attractive choice for these countries (Adee 2019). Second, the Chinese government seems an ideal partner for countries in need of competitively priced digital products and services, such as 5G mobile and cloud services (Erie and Streinz 2021). Through the DSR, China offers high-quality infrastructure and software at good prices to developing countries. It is estimated that the world's infrastructure financing gap will be nearly USD 15 trillion by 2040 (WEF 2019). DSR-related investment can contribute to filling that gap. By 2018, investment in digital infrastructure projects outside China within the DSR framework had reached USD 79 billion (Ghiasy and Krishnamurthy 2021). Moreover, through DSR-related projects, Chinese firms can boost cooperation between scientists and engineers in these countries and their Chinese counterparts by establishing training centres and developing research programmes (Council on Foreign Relations 2020). China's version of cyber governance, with its focus on sovereignty and multilateralism as well as its cost competitiveness, thus creates demand for Chinese cyber technology under the framework of DSR.

Countries within the Western bloc show more resistance to China's cyber norms. The Atlantic Council's Jason Healey (2011) calls this divergence "a bifurcation between east and west", which leads to limited possibilities for cooperation. Western bloc countries have consistently criticised China's cyber norms. For example, US Assistant Secretary for Communications and Information Lawrence Strickling (2015) criticised China's cyber governance approach for pursuing more control over cyberspace.

Nevertheless, the dichotomy between China's state-led, sovereignty-oriented approach and the West's more open approach is more blurred than it may appear. Many countries, including some from the West, have placed increasing emphasis on intergovernmental involvement and data sovereignty to protect their own markets from US and Chinese technology giants (Moynihan and Patel 2021). As highlighted above, the EU believes that digital sovereignty is necessary for an ensured role of sovereign governments and to counterbalance the hegemonic role of the US in cyberspace and obtain digital autonomy.

Even so, there are fundamental differences between the EU's and China's approaches to cyber governance, above all, a dispute on the meaning of cyber sovereignty. China's promotion of cyber sovereignty is driven more by national security concerns than the desire to protect personal information. In comparison, the EU's pursuit of sovereignty in cyberspace is motivated by the protection of public rights, such as data privacy, and the development of a European digital economy. Moreover, although the EU has stressed the importance of government involvement, it supports the multi-stakeholder model rather than the multilateral model. Despite these fundamental differences between the EU's digital sovereignty and China's cyber sovereignty, Brussels might arguably serve as a mediator in US–China cyber disputes, facilitating a possible convergence between the US and the Chinese approaches.

Conclusion and implications

To provide a timely reflection on the new dynamics of global cyber governance, this article has drawn on the concept of norm entrepreneur to develop an empirically grounded analysis of China's role as a norm entrepreneur.

By examining the principal norms guiding China's cyber practices, China's attempts at establishing its cyber norms and the extent to which these norms have been accepted or not by other countries, the article overcomes the false dichotomy of the West vs. non-West debate over global cyber governance and makes two contributions to the literature on cyber norm entrepreneurs. First, it moves beyond the conventional cyber sovereignty framework to offer a comprehensive understanding of China's cyber governance approach. It argues that, although Beijing puts cyber sovereignty and government involvement at the core of its cyber governance approach, China's Internet policies are a result of interactions between state agencies and business units, and recent reforms demonstrate the possibility of greater involvement by Chinese companies.

Second, this research looks into how divergence over cyber norms within the Western bloc may lead to different levels of receptiveness to China's cyber norms. It is not surprising that China's sovereignty narrative is attractive to emerging cyber powers as well as small and mid-size cyber players, because the Chinese government may appear to be an ideal partner for countries seeking to challenge the US hegemony and needing competitively priced digital products and services. The blurring of the dichotomy between China's sovereignty-oriented approach and the more open approach promoted by Western countries may lead to the latter becoming more receptive to China's cyber norms. In particular, despite fundamental differences between the EU's digital sovereignty and China's cyber sovereignty, Brussels might arguably facilitate a possible convergence between the Western approach and China's sovereignty-oriented approach.

Notes on contributor

Xinchuchu Gao is a Teaching Fellow in European Political Economy at the London School of Economics and Political Science and a Visiting Research Fellow at the London Asia-Pacific Centre for Social Science at King's College London, both in London, United Kingdom.

References

Adamson, Liisi, and Homburger, Zine. 2019. Let Them Roar: Small States as Cyber Norm Entrepreneurs. *European Foreign Affairs Review* 24 (2): 217-34.

Adee, Sally. 2019. The Global Internet is Disintegrating – What Comes Next? *BBC*, 15 May. https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

Anagnostakis, Dimitrios. 2021. The European Union-United States Cybersecurity Relationship: A Transatlantic Functional Cooperation. *Journal of Cyber Policy* 6 (2): 243-61.

Bhuiyan, Abu. 2014. *Internet Governance and the Global South: Demand for a New Framework*. Basingstoke: Palgrave Macmillan.

BRICS Summit. 2017. Full Text of BRICS Leaders Xiamen Declaration. 4 September. http://www.brics.utoronto.ca/docs/170904-xiamen.html.

Broeders, Dennis, and Van Den Berg, Bibi, eds. 2020. *Governing Cyberspace: Behavior, Power and Diplomacy*. London: Rowman & Littlefield Publishers.

Bull, Benedicte, Boas, Morten, and McNeill, Desmond. 2004. Private Sector Influence in the Multilateral System: A Changing Structure of World Governance. *Global Governance* 10 (4): 481-98.

Cai, Cuihong. 2018. Global Cyber Governance: China's Contribution and Approach. *China Quarterly of International Strategic Studies* 4 (01): 55-76.

Chen, Xuechen, and Yang, Yifan. 2022. Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance. *The International Spectator*, forthcoming.

Cheney, Clayton. 2019. China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. *Issues & Insights* 19 (WP8). https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf.

China's State Council. 2021. 国家标准化发展纲要 [National Strategy for Technical Standards]. 10 October. http://www.gov.cn/zhengce/2021-10/10/content_5641727.htm.

Christou, George. 2014. The EU's Approach to Cyber Security. *EU-China Security Cooperation: Performance and Prospects Policy Paper Series*. EUSC, 2 December. https://www.essex.ac.uk/research-projects/eu-china-security-cooperation/publications.

Clendenin, Mike. 2006. ISO Rejects China's WLAN Standards. *Electronic Engineering Times*, 3 December. https://www.eetimes.com/document.asp?doc_id=1159974.

CNNIC. 2021. 第47次《中国互联网络发展状况统计报告》 [The 47th Statistical Report on the Development of Internet in China]. 3 February. http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202102/t20210203_71361.htm.

Council on Foreign Relations. 2020. Assessing China Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms? https://www.cfr.org/china-digital-silk-road/.

Crandall, Matthew, and Allan, Collin 2015. Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms. *Contemporary Security Policy* 36 (2): 346-68.

Creemers, Rogier. 2020. China's Conception of Cyber Sovereignty. In Dennis Broeders and Bibi Van Den Berg, eds. 2020. *Governing Cyberspace: Behavior, Power and Diplomacy*: 107-42. London: Rowman & Littlefield Publishers.

Crovitz, L. Gordon. 2012. America's First Big Digital Defeat. *The Wall Street Journal*, 16 December. http://online.wsj.com/news/articles/SB10001424127887323981504578181533577508260.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven (CT)-London: Yale University Press.

DeNardis, Laura. 2020. *The Internet in Everything: Freedom and Security in a World with No Off Switch*. New Haven (CT): Yale University.

Dunn Cavelty, Myriam. 2018. Europe's Cyber-power. *European Politics and Society* 19 (3): 304-20.

Emmanuel Macron. 2020. Speech of the President of the Republic on the Defense and Deterrence Strategy. 7 February. https://www.elysee.fr/en/emmanuel-macron/2020/02/07/speech-of-the-president-of-the-republic-on-the-defense-and-deterrence-strategy.

Erie, Matthew S., and Streinz, Thomas. 2021. The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance. *54 N.Y.U.J. Int'l L. & Pol.* 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3810256.

European Parliament. 2020a. Together for Europe's Recovery: Germany Takes over Council Presidency. https://www.europarl.europa.eu/news/en/headlines/eu-affairs/20200624STO81905/together-for-europe-s-recovery-germany-takes-over-council-presidency.

European Parliament. 2020b. Digital Sovereignty for Europe. *EPRS Ideas Paper: Towards a More Resilient EU*, July. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

Farrell, Henry, and Finnemore, Martha. 2013. The End of Hypocrisy: American Foreign Policy in The Age of Leaks. *Foreign Affairs* 92 (6): 22-6.

Finnemore, Martha, and Hollis, Duncan B. 2016. Constructing Norms for Global Cybersecurity. *American Journal of International Law* 110 (3): 425-79.

Finnemore, Martha, and Sikkink, Kathryn. 1998. International Norm Dynamics and Political Change. *International Organization* 52 (4): 887-917.

G7. 2021. G7 Roadmap for Cooperation on Data Free Flow with Trust. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986160/Annex_2__Roadmap_for_cooperation_on_Data_Free_Flow_with_Trust.pdf.

Ghiasy, Richard, and Krishnamurthy, Rajeshwari. 2020. China's Digital Silk Road—Strategic Implications for the EU and India. *Special Report* 208. IPCS-Leiden Asia Centre, August. http://www.ipcs.org/issue_select.php?recNo=6153.

Ghiasy, Richard, and Krishnamurthy, Rajeshwari. 2021. China's Digital Silk Road and the Global Digital Order. *The Diplomat*, 13 April. https://thediplomat.com/2021/04/chinas-digital-silk-road-and-the-global-digital-order/.

Glen, Carol M. 2021. Norm Entrepreneurship in Global Cybersecurity. *Politics & Policy* 49 (5): 1121-45.

Gong, Shen, and Li, Bingqin. 2019. The Digital Silk Road and the Sustainable Development Goals, *IDS Bulletin* 50 (4). DOI: 10.19088/1968-2019.137.

Hakmeh, Joyce. 2017. Building a Stronger International Legal Framework on Cybercrime. *Chatham House*, 6 June. https://www.chathamhouse.org/2017/06/building-stronger-international-legal-framework-cybercrime.

Healey, Jason. 2011. Comparing Norms for National Conduct in Cyberspace. *New Atlanticist*, 20 June. https://www.atlanticcouncil.org/blogs/new-atlanticist/comparing-norms-for-national-conduct-in-cyberspace/.

Hong, Yu, and Goodnight, G. Thomas. 2019. How to Think about Cyber Sovereignty: The Case of China. *Chinese Journal of Communication* 13 (1): 8-26.

Huang, Huikang. 2012. Statement at Budapest Conference on Cyber Issues. 4 October. https://www.fmprc.gov.cn/ce/cgvienna/eng/zgbd/t977627.htm.

Huang, Zhixiong 2016. China and Rule of Law in Cyberspace. In Liangjie Zeng and Jiehan Feng, eds. *Annual Report on China's Practice in Promoting the International Rule of Law*: 97-107. Social Science Academic Press, SSAP.

Hurel, Louise Marie, and Lobato, Luisa Cruz. 2018. Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs. *Journal of Cyber Policy 3* (1): 61-76.

Kennedy, Scott. 2006. The Political Economy of Standards Coalitions: Explaining China's Involvement in High-tech Standards Wars. *Asia Policy* 2 (1): 41-62.

Kim, Mi Jin, Lee, Heejin, and Kwak, Jooyoung. 2020. The Changing Patterns of China's International Standardization in ICT under Techno-Nationalism: A Reflection through 5G Standardization. *International Journal of Information Management* 54: 102145.

Liaropoulos, Andrew. 2016. Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics. *Journal of Information Warfare* 15 (4): 14-26.

Liu, Yangyue. 2012. The Rise of China and Global Internet Governance. *China Media Research* 8 (2): 46-55.

Lu, Wei. 2015. Cyber Sovereignty Must Rule Global Internet. *Huffington Post*, updated 14 February. https://www.huffpost.com/entry/china-cyber-sovereignty_b_6324060.

Maurer, Tim. 2011. Cyber Norm Emergence at the United Nations. *Discussion Paper* 2011-11. Cambridge (MA): Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf.

Meltzer, Joshua P. 2020. China's Digital Services Trade and Data Governance: How Should the United States Respond? *Brookings*, October 2020. https://www.brookings.edu/articles/chinas-digital-services-trade-and-data-governance-how-should-the-united-states-respond/.

Ministry of Foreign Affairs of the People's Republic of China. 2017. International Strategy of Cooperation on Cyberspace. 2 March. https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.

Moynihan, Harriet, and Patel, Champa. 2021. Restrictions on Online Freedom of Expression in China. *Research Paper*. Chatham House, 17 March. https://www.chathamhouse.org/2021/03/restrictions-online-freedom-expression-china.

O'Hara, Kieron, and Hall, Wendy. 2018. Four Internets: The Geopolitics of Digital Governance. *CIGI Papers* No. 206. https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance/.

Office of the Central Cyberspace Affairs Commission. 2018.《"一带一路"数字经济国际合作倡议》发布 [Launch of the "Belt and Road" Digital Economy International Cooperation Initiative]. 11 May. http://www.cac.gov.cn/2018-05/11/c_1122775756.htm.

Office of the Leading Small Group for Promoting the Work of Constructing the "Belt and Road Initiative". 2019. 共建"一带一路"倡议:进展、 贡献与展望 [Jointly Sponsor the "Belt and Road Initiative": Progress, Contribution, and Prospects]. 22 April. http://www.xinhuanet.com/world/2019-04/22/c_1124400071.htm.

Pohle, Julia, and Thiel, Thorsten. 2020. Digital Sovereignty. *Internet Policy Review* 9 (4): 1-19.

Qiushi. 2017. 深入贯彻习近平总书记网络强国战略思想 扎实推进网络安全和信息化工作 [In-Depth Implementation of General Secretary Xi Jinping's Strategic Thinking on Strengthening the Country through the Internet, and Solid Progress in Network Security and Information]. 15 September. http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm.

Raymond, Mark, and DeNardis, Laura. 2015. Multistakeholderism: Anatomy of an Inchoate Global Institution. *International Theory* 7 (3): 572-616.

Rebello, Katarina. 2017. Building Walls with 'BRICS'? Rethinking Internet Governance and Normative Change in a Multipolar World. *Centre for Global Constitutionalism* 43 (2): 25.

Reddy, Latha, and Soni, Anoushka. 2021. Is There Space for a Digital Non-Aligned Movement? *Cyberstability Paper Series*. The Hague Centre for Strategic Studies and the Global Commission on the Stability of Cyberspace, 30 September. https://hcss.nl/report/is-there-space-for-a-digital-non-aligned-movement/.

Rõigas, Henry. 2015. An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New? https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/.

SCIO (State Council Information Office). 2010. White Paper on the Internet in China. 8 June. http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.

Scott, Mark. 2019. What's Driving Europe's New Aggressive Stance on Tech. *Politico*, 27 October. www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen.

Segal, Adam. 2020. China's Alternative Cyber Governance Regime. Prepared Statement. Council on Foreign Relations, 13 March. https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

Sheehan, Matt, Blumenthal, Marjory, and Nelson, Michael R. 2021. Three Takeaways from China's New Standards Strategy. *Carnegie Endowment*, 28 October. https://carnegieendowment.org/2021/10/28/three-takeaways-from-china-s-new-standards-strategy-pub-85678.

Shen, Hong. 2016. China and Global Internet Governance: Toward an Alternative Analytical Framework. *Chinese Journal of Communication* 9 (3): 304-24.

Si, Ma. 2020. Huawei Secures Most 5G Contracts around World. *China Daily*, 22 February. https://www.chinadaily.com.cn/a/202002/22/WS5e50491ea3101282172796b9.html

Stevens, Tim. 2012. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy* 33 (1): 148-70.

Strickling, Lawrence E. 2015. Internet Governance Progress After ICANN 53: Hearing Before Subcommittee on Communications and Technology Committee on Energy and Commerce, United States House of Representatives. https://www.govinfo.gov/content/pkg/CHRG-114hhrg97750/pdf/CHRG-114hhrg97750.pdf.

Taylor, Emily, and Hoffmann, Stacie. 2019. EU-US Relations on Internet Governance. *Research Paper*. Chatham House, November. https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf.

The Chinese Representative. 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://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

UNCTAD (United Nations Conference on Trade and Development). 2019. Digital Economy Report 2019. Value Creation and Capture: Implications for Developing Countries. https://unctad.org/system/files/official-document/der2019_en.pdf.

WEF (World Economic Forum). 2019. The World Is Facing a $15 Trillion Infrastructure Gap by 2040. Here's How to Bridge It. 11 April. https://www.weforum.org/agenda/2019/04/infrastructure-gap-heres-how-to-solve-it/.

White House. 2014. Fact Sheet: U.S.—EU Cyber Cooperation. 26 March. https://obamawhitehouse.archives.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.

Woetzel, Jonathan, *et al.* 2017. China's Digital Economy: A Leading Global Force. *Discussion Paper*. McKinsey Global Institute, August. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/China/Chinas%20digital%20economy%20A%20leading%20global%20force/MGI-Chinas-digital-economy-A-leading-global-force.ashx.

Xi Jinping. 2015. 习近平在第二次世界互联网大会的讲话全文 [Remarks by H.E. Xi Jinping President of the People's Republic of China at the Opening Ceremony of the Second World Internet Conference]. 16 December. http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm.

Xinhua. 2020. Economic Watch: China Advances Digital Trade to Fuel Economic Growth. 7 September. http://www.xinhuanet.com/english/2020-09/07/c_139349050.htm.

Zeng, Jinghan, Stevens, Tim, and Chen, Yaru. 2017. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics and Policy* 45 (3): 432-64.

Zhao, Yuezhi. 2010. China's Pursuits of Indigenous Innovations in Information Technology Developments: Hopes, Follies and Uncertainties. *Chinese Journal of Communication* 3 (3): 266-89.

Zhaoxiong, Chen. 2019. "推动工业和信息化高质量发展" [Promote the High-Quality Development of Industry and Informatization]. *Renmin*, 8 July. http://theory.people.com.cn/n1/2019/0708/c40531-31221197.html.

Zhengzhong, Xu. 2020. 网络空间治理的任务与挑战 [The Tasks and Challenges of Network Space Governance]. *Party & Government Forum* 1: 36-37.

Zipser, Daniel, and Poh, Felix. 2021. Understanding Chinese Consumers: Growth Engine of the World. *China Consumer Report* 2021. McKinsey & Company, November. https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20still%20the%20worlds%20growth%20engine%20after%20covid%2019/mckinsey%20china%20consumer%20report%202021.pdf.