Common destiny in cyberspace: China's cyber diplomacy

Creemers, R.J.E.H.; Pieke, F.N.; Iwabushi, K.

TWENTY-ONE

Common Destiny in Cyberspace

CHINA'S CYBER DIPLOMACY

Rogier Creemers

ONE OF THE MOST CLOSELY observed elements of China's social and political transformation over the past decade has been the digital sphere. However, China's growing international footprint, its engagement with emerging regimes for global cyber governance, and its own diplomatic efforts have remained out of the academic limelight. Until around 2013, China did not play a role of great significance in global cyber-related processes and did not have a well-developed policy agenda of its own, nor dedicated institutions to support it. Between 2001 and 2009, China boycotted the Governmental Advisory Committee of the International Corporation for Assigned Names and Numbers (ICANN), the authority in charge of the internet's addressing system.[1] In some of the earliest iterations of the UN Group of Governmental Experts (GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security, China sent officials, who were less versed in the legal and security questions from its ministry of communication.[2]

Across a swathe of issue areas, China's foreign engagement remains limited. Together with Russia, it formed the core of a "coalition of the unwilling," a group of states united primarily in their rejection of what they perceived as an emerging American hegemony in cyberspace. Opposing US notions of a free and open internet governed by universal principles and values, they proposed sovereignty as the fundamental norm, and argued cyber affairs were a matter of national sovereignty. International coordination and cooperation between states should take place through UN channels, instead of using the multistakeholder model advocated by the West and practiced by institutions such as ICANN.

From 2013 onward, however, questions concerning cyber security and internet governance rapidly gained political prominence, as successive events

demonstrated the severity of the challenge China faced. Many of these challenges, such as the proliferation of political activism on social media and online scamming, were primarily domestic in nature. Yet at the same time, incidents such as the Edward Snowden revelations and Microsoft's discontinuation of security support for Windows XP, as well as increasing tensions over cyber espionage, hacking, technology transfer, and intellectual property infringement, caused a new degree of awareness of risks from abroad, and particularly from the United States. In response, President Xi Jinping called for China to become a "cyber power."[3] To this end, both institutional and policy moves were made. A new top-level leadership organ, the Central Leading Group (later, Central Commission) for Cybersecurity and Informatization, came into being in 2014. Chaired by Xi personally, it included senior officials from propaganda, telecommunications, and technology ministries, as well as from the military. The State Internet Information Office, later renamed the Cyberspace Administration of China (CAC), grew in capacity and importance, serving, among other things, as the coordination body for the Central Commission. Numerous policy and legal documents saw the light of day, including comprehensive plans for the digital sector and the 2017 Cybersecurity Law. For the first time, international questions were addressed directly, specifically in the Strategy for International Cooperation in Cyberspace,[4] as well as through initiatives such as the Wuzhen World Internet Conference (WIC) and the Digital Silk Road (DSR). The latter provided a technological supplement to the flagship Belt Road Initiative.

CYBER GOVERNANCE AND CYBER SOVEREIGNTY

China's international cyber policies are predominantly shaped by its core domestic concerns: economic development and political stability. The prime international adversary is the United States, and the escalating tensions between these two countries concerning technology reflect growing opposition in the broader relationship. Put succinctly, China's leadership fears that the United States is determined to halt China's justified process of rejuvenation in its tracks, consigning the country to a permanent subordinate status. American positions and measures in cyberspace are usually interpreted in that light. Under the Obama administration, Secretary of State Hillary Clinton's open internet agenda, for instance, was portrayed as a direct challenge to China's ideological security. ICANN's past subordination to a US

Department of Commerce mandate was seen as giving the United States control over the strategic infrastructure of the internet. The Snowden revelations spurred anxiety about the extent to which China's reliance on foreign technologies created vulnerabilities.

Chinese policies have been largely reactive to these concerns, aiming to build "discursive power" in global cyber governance circles and to increase self-reliance in technology. In its search for discursive power, China's 2017 International Strategy of Cooperation on Cyberspace lists four fundamental principles: peace, sovereignty, shared governance, and mutual benefit. China rejects the use of cyberspace for military applications, even if it is currently developing defensive cyber forces. It also calls for collaboration in the fight against terrorists' use of the internet.

The most fundamental, yet controversial, principle is cyber sovereignty. Cyber sovereignty rejects the universality of political values and constitutional principles. Instead, China asserts that all countries have the right to govern the internet within their jurisdiction as they see fit, and to decide on their own technological development path. It assumes that borders exist in cyberspace as they do in real space. It is the prerogative of governments to police those borders and regulate the activities taking place within them. Sovereignty is primarily framed as noninterference and the right to self-determination: no fundamental values, such as free speech rights, outrank governmental power, nor should countries support the defense of such values outside their own borders. This assumption delineates what "shared governance" refers to in this context, as sovereignty also implies the supremacy of the state over nonstate actors.[5]

In contrast to the Western emphasis on multistakeholder governance of the internet, China proposes a "multiparty" model, in which governments and international governmental organizations take the lead, businesses, trade associations, and the technical community contribute specific expertise, and civil society is mentioned last.[6] Such cooperation should take place on the basis of mutual benefit—that is, efforts should be directed to making digital technology an engine for global growth and development. Together, according to Xi Jinping, the principles of cyber sovereignty, the multiparty model, and mutual benefit will combine to create a "community of common destiny in cyberspace."

These principles are important at the level of symbols and rhetoric: one of China's key objectives has been to insert these concepts into international normative documents on cyber governance and to persuade foreign actors,

including governments, to adopt them. They have been accompanied by a push to expand China's footprint on the ground, most notably through growing the international market share of China's technology businesses, increasing the proportion of indigenous content in international technology standards, and incorporating technology cooperation in China's foreign development assistance.

DIGITAL SILK ROAD

China's "Silk Road Economic Belt" was announced in 2013. Later rebranded as "One Belt One Road," and still later as the "Belt and Road Initiative" (BRI), it was originally focused primarily on traditional forms of connectivity. Gradually, digital technologies entered into the plan. The 2016 thirteenth Five-Year Plan for National Informatization, for instance, contained a dedicated section on the "Online Silk Road." At the first BRI forum in Beijing in 2017, Xi Jinping underlined the importance of new forms of technology for innovation-driven development, including artificial intelligence, big data, cloud computing, and smart cities. As with the overall BRI scheme, goals of the Digital Silk Road include mitigating China's overcapacity problems, opening up new markets for national champions, and supporting the internationalization of the renminbi.[7] In some cases, digital technology is required for broader BRI objectives, such as satellite navigation for infrastructure construction. More specifically, the Digital Silk Road also contains elements intended to further China's cyber agenda, through building support in third countries and enhancing the clout and influence of its businesses. Like the BRI, the Digital Silk Road is not a sharply delineated project. Consequently, businesses, research institutions and governmental bodies regularly use the term as a politically convenient description for projects they are doing anyway, or to attract support and subsidies.

A first major Digital Silk Road element is the international adoption of Chinese technologies, ranging from telecommunications infrastructure and mobile handsets to satellite navigation and smart traffic control. This, it is hoped, will enable Chinese businesses not only to increase profitability but will also ensure that their technologies are incorporated in international standards and complex value chains. The highest profile effort is the attempt to include technologies developed by businesses such as ZTE and Huawei into standards for fifth-generation (5G) mobile telecommunications. Owing

to rising national security concerns, both companies face increasing headwinds in developed markets. Intelligence agencies from the "Five Eyes" have reportedly decided to contain Huawei's growth.[8] The United States, Australia, and New Zealand have all banned Huawei from their market. The United Kingdom, Germany, and Belgium have launched security investigations into the potential risk posed by Huawei technologies but, as of May 2019, have as yet stopped short of an all-out ban. Huawei's chief financial officer, Meng Wanzhou, was arrested in Canada at the behest of the United States in December 2018. In subsequent months, tensions concerning Huawei escalated, leading to the US government imposing an export ban against Huawei in May 2019. China's cyber strategy is now at the core of the escalating conflict and the rivalry between China and the United States, as well as, increasingly and more broadly, with all major Western powers. A greater Chinese presence in third countries, such as Belt and Road nations, may mitigate China's exposure to further measures from Western powers and provide it with potential allies in future trade disputes.

In the area of satellite navigation, China has identified the Central Asian section of the BRI as the first major internationalization zone for its Beidou program, an alternative for the American Global Positioning System (GPS) and the European Galileo system. To this end, China has reached agreement with a number of countries on their military use of Beidou, while an industrial park for Sino-Arab satellite data services was established in Ningxia.[9] For recipient countries, Beidou may be attractive in order to hedge their reliance on GPS, even if only as a fallback option.

Secondly, China has used the Digital Silk Road as a platform for diplomatic engagement aimed at cooperation in the digital economy. At the 2017 Wuzhen conference, Saudi Arabia, Egypt, Turkey, Thailand, Laos, Serbia, and the UAE signed an agreement with China for an economically interconnected DSR.[10] The agreement included matters like expanding broadband connectivity and cooperation in international standardization. Perhaps more importantly, the countries also promised to work on the harmonization of e-commerce and data protection-related laws. Nonetheless, little fanfare accompanied this agreement. This, and the fact that it was circulated widely for several months, including among EU governments, suggest that the leadership had anticipated greater adoption. Foreign governments have remained doubtful about the business practices of Chinese companies and good governance issues where BRI and Digital Silk Road projects are concerned.

Given the relatively early stage of the Digital Silk Road, it currently remains largely speculative whether the project will contribute to Beijing's foreign policy goals in the short and long term. Moreover, Chinese actors have used the Digital Silk Road banner to tout projects and processes already underway. Kuala Lumpur, for instance, has purchased Alibaba's City Brain technology for urban management.[11] A major fiber-optic network has been completed in Afghanistan and will be run jointly by Afghan Telecom and China Telecom.[12] Chinese businesses have enjoyed considerable growth in e-commerce in South-East Asia and have established data centers along the Belt and Road. These projects do not necessarily require BRI support as they make commercial sense on their own. They have, however, provided opportunities to the businesses conducting them in order to get into Beijing's good books.

IMPLICATIONS

If the objective of China's foreign cyber policy has been to acquire greater acceptance of its stance, or at least a greater supporting coalition, there is little doubt that they have been largely unsuccessful so far. To a certain degree, this reflects the broader state of affairs in cyberspace, which is primarily caused by the continuing and deepening tensions between the United States and the "like-minded countries," on the one hand, and Russia and China, on the other. But even with countries farther removed from the US orbit, China is not faring very well, as the limited take-up of the Digital Silk Road initiative demonstrates. China has not yet managed the transition from a relatively small and insignificant player to a global leader. China's cyber policies have become slightly more elaborate but they remain largely programmatic and, to a certain degree, inconsistent. China may also have failed to generate sufficient trust among its potential foreign partners. Concerns about matters ranging from expanding surveillance and censorship to hacking and intellectual property rights infringement, to the real or perceived potential of espionage through China-backed infrastructure rapidly become more prominent in international discourse. To allay these fears, China would have to become more transparent about its policy mechanisms and intentions, and Chinese businesses would have to allow closer scrutiny.

Yet China's view of the world and policy approach may leave little space for foreign input. The Digital Silk Road is focused primarily on solving

Chinese domestic problems, even if it is packaged as a foreign aid and development project. With little room for target countries to develop their own tech industries, combined with the risks connected with indebtedness to China, the Digital Silk Road might therefore be less attractive than Beijing believes. The best—but unlikely—response would be for Beijing to relinquish absolute control over these processes and allow meaningful external participation in DSR-related decision-making.

These points raise two bigger questions. The first is to what extent Beijing will learn from its experiences in foreign affairs. The Chinese Communist Party prides itself on being a "learning party." With relatively little experience in leadership in complex geopolitical questions, a considerable amount of learning likely awaits. Together with climate change, the cyber domain is one of the most prominent issue areas in which China's newly found international assertiveness manifests itself. The extent to which Beijing digests, internalizes, and applies the lessons it learns through its policy experience will thus more broadly be a useful guide to China's evolving position in the global order. The second question is how the outside world will respond to China's ambitions. Increasing tensions between the United States and China have led to what some observers on both sides are already calling the "Sino-US Tech Cold War." If this trend continues, it may have major implications not just for the global internet but for global trade and geostrategic questions as well.

NOTES

1. Cheng 2017, 61.
2. Segal 2017.
3. Xi Jinping. "Ba woguo cong wangluo daguo jianshe chengwei wangluo qiangguo" [Build our country from a large network country into a strong network country], Xinhua, February 27, 2014, http://www.xinhuanet.com//politics/2014-02/27/c_119538788.htm.
4. Foreign Ministry of the People's Republic of China (FMPRC) 2017.
5. Schia and Gjesvik 2017.
6. Ministry of Foreign Affairs,, "International Strategy of Cooperation on Cyberspace," trans. Rogier Creemers, March 1, 2017, https://chinacopyrightandmedia.wordpress.com/2017/03/01/international-strategy-of-cooperation-on-cyberspace/.
7. Shen 2018.
8. The "Five Eyes" is an intelligence alliance comprising the United States, the United Kingdom, Canada, Australia, and New Zealand. See Chris Uhlmann and

Angus Grigg, "Secret Meeting Led to the International Effort to Stop China's Cyber Espionage," *Financial Review*, December 13, 2018. https://www.afr.com/world/asia/secret-meeting-led-to-the-international-effort-to-stop-chinas-cyber-espionage-20181213-h192ky.

9. Wu 2015.

10. Rogier Creemers, "Proposal for International Cooperation on the 'One Belt, One Road' Digital Economy" (proposed international agreement presented at the World Internet Conference, Wuzhen, Zheijiang, China, December 3, 2017).

11. Abigail Beall, "In China, Alibaba's Data-hungry AI Is Controlling (and Watching) Cities," *Wired*, May 30, 2018, https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur.

12. Rachel Brown, "Beijing's Silk Road Goes Digital," Council on Foreign Relations, June 6, 2017, https://www.cfr.org/blog/beijings-silk-road-goes-digital.

REFERENCES AND FURTHER READING

Cheng, Dean. 2017. *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*. Santa Barbara, CA: Praeger International Security.

Foreign Ministry of the People's Republic of China. 2017. "Wangluo kongjian guoji hezuo zhanlüe" [International strategy of cooperation on cyberspace]. China Copyright and Media. March 1, 2017. https://chinacopyrightandmedia.wordpress.com/2017/03/01/international-strategy-of-cooperation-on-cyberspace/.

Schia, Niels Nagelhus, and Lars Gjesvik. 2017. "China's Cyber Sovereignty." Norwegian Institute of International Affairs. March 17, 2017. https://www.nupi.no/en/Publications/CRIStin-Pub/China-s-Cyber-Sovereignty.

Segal, Adam. 2017. "Chinese Cyber Diplomacy in a New Era of Uncertainty." Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, no. 1703. June 2, 2017. http://lawfareblog.com/chinese-cyber-diplomacy-new-era-uncertainty.

Shen, Hong. 2018. "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative." *International Journal of Communication* 12 (June): 2683–701.

Wu, Sike. 2015. "Constructing 'One Belt and One Road' and Enhancing the China-GCC Cooperation." *Journal of Middle Eastern and Islamic Studies (in Asia)* 9, no. 2: 1–15.