China, Law and Development

RESEARCH BRIEF No. 14/2020

The Digital Silk Road and China's Role in the UN Ad Hoc Cybercrime Committee

Jacob Skebba
Peking University
November 24, 2020

Key Points:

- The BRI may be best known for large infrastructure projects in the energy and transportation sectors, but for the last several years it has increasingly focused on digital infrastructure. The coronavirus pandemic is likely to further encourage this focus.
- The digital infrastructure component of the BRI not only includes projects developing the physical infrastructure to support digitization in host countries; it also extends to the development of "softer" infrastructure, including work on international digital governance frameworks.
- A relatively high-profile example of this governance work going forward could be China's participation in a UN committee charged with discussing cyberspace norms and possibly developing a new cybersecurity treaty. Participation in drafting such a treaty could be an important component of the Digital Silk Road, but the treaty drafting process is currently at a very early stage and it remains to be seen what role China will play in the committee.

Introduction

China's Belt and Road Initiative (BRI) was originally conceived as a massive infrastructure project intended, at least in part, to connect China to emerging markets throughout Asia and beyond. While a focus on infrastructure has remained as the BRI has matured, the concept of infrastructure has evolved to keep pace with China's capabilities and host countries' needs. In particular, the BRI has expanded to include digital infrastructure, with official recognition of the role digital infrastructure plays in the BRI beginning as early as 2015 when talk of a "Digital Silk Road" began.

While the involvement of Chinese technology companies beyond China's borders long predates official recognition of the Digital Silk Road as a component of the BRI, political recognition and government backing have likely expanded one particular component of the Digital Silk Road: the involvement of both the Chinese government as well as private Chinese companies in international policymaking in the digital realm. This Research Brief briefly describes the growth of the Digital

Silk Road, including its policymaking component, before discussing China's potential role in emerging multilateral efforts to address the increasingly prominent cybersecurity challenges that accompany digital development.

The Digital Silk Road

The specific concept of the Digital Silk Road may be relatively new, but China's technology companies have operated in emerging markets for much longer, beginning even before their activities could fall under the broad umbrella of the BRI. Accordingly, the Digital Silk Road is probably best seen less an initiative consisting of entirely new activities and more a branding exercise that brings existing activities into the BRI while offering state support for further expansion and coordination. The intent to expand the export of digital infrastructure and services under the auspices of the state through the BRI seems apparent based on Beijing's recent focus on digital issues when discussing the BRI. For example, Beijing has specifically promoted the Digital Silk Road in recent years at the Second Belt and Road Forum, the 5th Wuhan Internet Conference, and other international fora.[1] In particular, the Second Belt and Road Forum featured a distinct sub-forum on the Digital Silk Road and drew attendees from over 30 countries.[2] Multilateral institutions associated with the BRI have also started to shift their focus towards digital infrastructure. For example, the Asian Infrastructure Investment Bank released a new digital strategy in June 2020 that contemplates increasing near-term investment in "hard" digital infrastructure while reserving the possibility of funding "soft" digital infrastructure as well, albeit possibly over a longer timeline.[3]

Making digital infrastructure development a core component of the BRI makes a lot of sense, particularly in the current development environment. While development-focused institutions had already been providing significant support for digital infrastructure development even before the emergence of the coronavirus pandemic, the demand for digital infrastructure investment is likely to further increase as a result of the pandemic.[4] Furthermore, digital infrastructure projects often have the added benefit of either mitigating or entirely sidestepping some of the concerns commonly raised by other BRI projects. For example, digital infrastructure projects are often cheaper and have a smaller footprint than other infrastructure projects (particularly transportation and energy projects), leading to comparatively fewer problems with host country debt and environmental and social impacts. By way of example, Huawei was able to complete an 820km fiber-optic cable project in Pakistan at less cost than it takes to build four kilometers of railway track while simultaneously avoiding some of the delays affecting other BRI projects in Pakistan.[5] Given that digital infrastructure projects still provide China with many of the same benefits as

[1] EURASIA GROUP, THE DIGITAL SILK ROAD: EXPANDING CHINA'S DIGITAL FOOTPRINT 3 (2020), https://www.eurasiagroup.net/live-post/digital-silk-road-expanding-china-digital-footprint.
[2] *Id.*
[3] ASIAN INFRASTRUCTURE INVESTMENT BANK, DIGITAL INFRASTRUCTURE SECTOR STRATEGY: AIIB'S ROLE IN THE GROWTH OF THE DIGITAL ECONOMY IN THE 21ST CENTURY (2020).
[4] Jude Blanchette & Jonathan E. Hillman, *China's Digital Silk Road after the Coronavirus* (Apr. 13, 2020), https://www.csis.org/analysis/chinas-digital-silk-road-after-coronavirus.
[5] *Id.*

more expensive, more difficult projects,[6] the increased focus on digital infrastructure should not come as a surprise.

Governance and the Digital Silk Road

It is worth noting that the Digital Silk Road is not limited to the development of hard digital infrastructure, however. It contemplates developing a legal and policy infrastructure for governing the digital world as well. Like Chinese development of digital infrastructure abroad, Chinese participation in international policymaking with regard to technology is not new. Chinese companies were involved in the development of international technological standards even before their work began to fall under the Digital Silk Road brand.[7] With increasing state attention and a growing market share for Chinese technology companies, Chinese influence at organizations like the International Telecommunication Union is likely to further grow in the years ahead.[8] Chinese participation in international policymaking is not limited to the development of technological standards either. China has also been actively promoting its concept of cybersovereignty in discussions of internet governance.[9] Cybersovereignty in general involves each state exerting greater control over the internet traffic passing within its borders, at least compared to the more open internet favored by western democracies.[10]

While an increased focus on digital infrastructure development has many benefits, it is not without its own unique issues. In particular, digital infrastructure development creates new security risks and attendant opportunities for cybercriminals and cyberterrorists. While cybercrime is a global problem, it is of particular concern in developing countries. Developing countries now account for over 70% of internet users, and the relative lack of state capacity for dealing with cybercrime places developing countries and their people at heightened risk.[11] The lack of state capacity in developing countries also presents risks for developed countries, as cybercriminals can exploit this dynamic by launching attacks from developing countries with low capacity.[12] Cybercrime thus presents a global problem, particularly given its blurring of national boundaries, and there are multiple concurrent attempts to address it on a multinational level. The newest attempt to do so involves the formation of an ad hoc cybercrime committee at the UN, which may eventually draft a new cybersecurity treaty.[13]

---

[6] *See* Hong Shen, *Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative*, 12 INT'L J. COMM. STUD. 2683, 2694 (2018) ("In China's policy discourse, a digital Silk Road has five major dimensions. The state hopes that assigning its native digital players a prominent role in BRI can mitigate industrial overcapacity, facilitate other Chinese firms' global expansion, support the internationalization of the renminbi, construct a China centered transnational network infrastructure, and promote an Internet-enabled inclusive globalization.").

[7] Robert Greene & Paul Triolo, *Will China Control the Global Internet Via its Digital Silk Road?,* CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, (May 8, 2020), https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857 .

[8] *Id.*

[9] *See, e.g.,* Samm Sacks, *Beijing Wants to Rewrite the Rules of the Internet*, THE ATLANTIC (June 18, 2018), https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

[10] Adam Segal, *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace* in An Emerging China Centric Order: China's Vision for a New World Order in Practice 87 (Nadège Rolland ed., 2020).

[11] JOANNA SWIATKOWSKA, TACKLING CYBERCRIME TO UNLEASH DEVELOPING COUNTRIES' DIGITAL POTENTIAL 18-19 (2020).

[12] *Id.*

[13] *See* G.A. Res. 74/247, U.N. Doc. A/RES/74/247 (Dec. 27, 2019).

Even though negotiations on the substantive portions of any new cybercrime treaty have yet to begin, the process so far reflects long standing differences between countries in their preferred approaches to addressing international cybersecurity in particular and international internet governance in general. The split can generally be described as being one between a camp that favors a multi-stakeholder approach and one that favors a state-centered, multilateral approach.[14] The former, favored by most western democracies including the United States, is an "approach to internet governance in which governments, private companies, civil society, the technical community and other independent organizations all have roles to play but in which no single entity operates without checks and balances."[15] The latter camp, promoted by Russia and China among others, involves a more top-down approach, where sovereign governments take the lead in developing internet governance rules and, comparatively speaking, each country has greater control of the internet within its own borders.

It was against this backdrop that the UN General Assembly adopted resolution 74/247 at the end of 2019 creating an ad hoc committee to potentially draft a new cybersecurity treaty. Russia was the original sponsor of the resolution, but it was also supported by China and several other countries. Since being proposed, however, the resolution, the process it proposes, and the draft treaty circulated by the Russians ahead of time have all drawn significant criticism. In particular, a group of civil society organizations published an open letter expressing their concerns.[16] Among their concerns are that the process proposed is, for now at least, primarily intergovernmental and leaves other stakeholders without a seat at the negotiating table.[17] It further notes that existing UN processes pre-dating the resolution calling for the formation of the ad hoc cybercrime committee are sufficient to develop an effective international cybersecurity framework and that a better route forward would be to update the Budapest Convention rather than draft an entirely new treaty.[18] These concerns regarding the approach to developing a new international internet governance framework were in addition to substantive concerns about the draft treaty circulated.[19] In any case, negotiations on a potential treaty itself have yet to begin and may end up taking an entirely different direction, but so far those countries favoring the state-centered approach seem to be gaining more traction than those favoring the multi-stakeholder approach.

While a multi-stakeholder approach in a strict sense would also be multilateral in that it would involve a number of sovereign states, a multilateral approach that prioritizes the input of governments and marginalizes other groups dovetails well with the concept of cybersovereignty. It therefore seems likely that China would continue to support this new push for a cybersecurity treaty at the UN beyond just co-sponsoring the resolution. So far, China has

[14] Henry L. Judy & David Satola, *Business Interests Under Attack in Cyberspace: Is International Regulation the Right Response?*, B.L. TODAY 1–5 (2011).
[15] *Id.*
[16] *Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online*, ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (Nov. 6, 2019), https://www.apc.org/en/pubs/open-letter-un-general-assembly-proposed-international-convention-cybercrime-poses-threat-human. .
[17] *Id.*
[18] *Id.*
[19] *Id.*

remained relatively distant from the process, however, choosing to sign on to a multinational comment on the proposed agenda rather than submitting their own comment as Russia, the United States, Japan, and several other countries have. Accordingly, the role China intends to take in the process is currently unclear. This of course may simply be a function of the fact that the process is still in a very early stage and is being further drawn out on account of the coronavirus pandemic. The organizational meeting for the ad hoc committee was originally scheduled to take place in August 2020 but has been pushed back and is now anticipated to take place no later than March 2021. It is further anticipated that the committee's work will be a multi-year process, scheduled to be completed in 2024. However, it may become clear much earlier (even as soon as the organizational meeting) what approach the committee intends to take and what role China intends to play in the committee deliberations.

Conclusion

China's increasing focus on digital infrastructure development offers many potential benefits both for China and for BRI host countries, and it is difficult to see it substantially slowing down in the near future. This rapid development of digital infrastructure presents some problems, however, particularly with regard to cybersecurity, and an ineffective or fractured global governance framework could prevent digital development from reaching its full potential. The development of digital infrastructure and the development of a framework to govern it are interdependent – developing digital infrastructure creates demand for effective governance, and effective governance will ideally prevent the negative externalities that may otherwise hinder the progress of digital development.

The Digital Silk Road recognizes this relationship and considers governance development an important component. Beyond simply facilitating digital development, however, participating in the development of cyberspace governance gives China an opportunity to promote its view of the ideal governing framework. Specifically, participating in international governance development provides the best opportunity for China to see cybersovereignty enshrined as a central principle of that governance.

Accordingly, the possible development of a new cybersecurity treaty is potentially of great importance to both digital infrastructure development in general and the goals of the Digital Silk Road in particular. The demand created by the continued development of digital infrastructure seems to ensure that digital governance will, if not become even more salient, at the very least remain a priority for the international community. An effective cybersecurity treaty may support the further development of digital infrastructure, but the process so far reflects deep divisions between different camps on which principles should underly the framework governing cyberspace. China's participation so far has been somewhat limited, but that may simply reflect the early stage of the process. Given the potential importance of a new treaty to the Digital Silk Road, it would not be surprising to see China play a prominent role as the process continues.

Jacob Skebba
Peking University
jacobskebba@stl.pku.edu.cn