JUNE 2020

BRIEF

CHINA'S SOVEREIGNTY AND INTERNET GOVERNANCE

KADRI KASKA | MARIA TOLPPA

China's readiness to impose itself and its determined actions to this end over the past decade can be seen in many areas, cyberspace certainly not the least of them. Despite a vocabulary similar to that used by the West, China's vision of cyberspace and its future differs quite fundamentally from Western interests and values. Therefore, we ask: If China is in pursuit of global power, what should we pay attention to? What should we consider and perhaps even worry about, in cyberspace?

CHINA'S DILEMMAS

China's economic and technological progress in recent decades has not gone unnoticed. The growth of its economic power goes hand in hand with growing political ambition and reach, the strategic direction, motives and dynamics of which have been somewhat surreptitious. In retrospect, we have to admit that it was only a matter of time before China's increased economic and political power led the country to attempt to alter the balance of power in cyberspace as well. With the world's largest number of internet users, a communications and innovation industry purposefully and effectively developed with government support, a share of profitable internet companies comparable to that of the US, and also significant military and intelligence capabilities in cyberspace, it should expect no less.

China's attitude towards cyberspace has been controversial: on the one hand the internet is welcomed by the country's official internet concept as a "crystallisation of human wisdom" and an enabler of innovation and economic success, and on the other it is treated with distrust.[1] Recalling the belief—or, depending on your point of view, the fear—that dominated the world as recently as at the beginning of the past decade (it's worth remembering the Arab Spring) that virtual space without borders would give birth to a new, borderless world order that would take power away from undemocratic governments, it could only have been expected that matters of internet regulation would be exceptionally politicised in China.

Unlike the Western technocratic approach, which has treated the internet primarily as a technological environment, China treats it above all as an information space that, to be protected from "subverting state power, undermining national unity [or] infringing upon national honour and interests", must be strictly organised and controlled by the government.[2] By conceding citizens' rights to freedom of expression and access to the internet, China emphasises its right under national sovereignty and jurisdiction to manage cyberspace within its borders by its own rules. China's "internet sovereignty" must be observed by all those that want to operate in the Chinese market, including global internet giants such as Google and Amazon.[3]

It is with reference to state sovereignty and the right to exercise jurisdiction within its borders that China justifies its extensive system of digital censorship. The world's most advanced technological and legal censorship framework, referred to as the Golden Shield or the "Great Firewall of China", has been broadened and improved especially since president Xi Jinping came to power in 2012; with the 2017 Cybersecurity Law, the entire internet policy has been centralised into the hands of the Cyberspace Administration of China.[4] Service providers have the duty to filter online content and block unwanted pages or queries, and the possibilities for anonymous web use are extremely limited.[5] The implementation of the new Social Credit System has led to the introduction of extensive surveillance,

particularly in respect of the Uyghur ethnic minority in the north-west of the country.[6]

China's vision of the fundamental problems of cyberspace is formulated in the country's International Strategy of Cooperation on Cyberspace. Noting that security and stability in cyberspace bears on the sovereignty, security and development interests of all countries, the current development of cyberspace is considered unbalanced, the rules inadequate and the order inequitable.[7] The strategy emphasises that countries should respect each other's right to choose their own path of cyber development, model of cyber-regulation and internet policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or undermine other countries' national security.[8]

Sovereign Superpower

At the 2017 Congress of the Communist Party of China, president Xi unveiled his plan to make China a "cyber-superpower". Xi presented the country's model of internet sovereignty as an alternative for countries that, "while promoting digital development, would still like to maintain their independence". The model is being exported to other countries, through technology and infrastructure as well as international norms, and in Africa and Latin America in particular, these efforts have met with some success.[9] China's approach to sovereignty cannot be overlooked in the context of the construction of the fibre-optic network known as the Digital Silk Road, a component of China's Belt and Road Initiative.[10]

Investments in infrastructure development associated with the construction of the Digital Silk Road will enable China to seek support for a number of its strategic interests. This provides an opportunity to increase the country's ability to develop new technologies and bring them to the market, thereby supporting the growth of China's economic weight on the global stage.[11] In addition, one of the elements of the Digital Silk Road is a remarkably active offensive of Chinese digital diplomacy—both in multilateral forums such as the International Telecommunication Union (ITU) and in bilateral relations with the countries targeted by the initiative. China is actively involved in the ITU's work through funding, technology and capability development, as it considers the ITU has a key role in achieving the UN's Sustainable Development Goals for 2030.[12] Finally, the right to speak that comes with infrastructure ownership supports China's endeavour in internet governance to concentrate more decision-making power in governments.

It is in many of the countries targeted for the Digital Silk Road initiative that criticism of the current multi-stakeholder model of governance falls on fertile ground: it is perceived that decision-making has moved disproportionately into the hands of Big Tech or the GAFAM companies (Google, Amazon, Facebook, Apple and Microsoft), and many, especially developing countries, are not happy about it.[13] In particular, given that the number of internet users in these countries is rapidly caching up with that of other continents, the greater is the expectation that equal consideration should be given to their interests and needs. Yet the West—albeit sensing the problems of today's cyberspace, such as the spread of false information and propaganda and the retreat of knowledge in the face of commercial interests—rejects a model in which infrastructure creators and owners and technology visionaries are reduced from being among the decision-makers for the future of cyberspace to executors of political orders from governments.

Two of China's strategic goals in global cyberspace are particularly difficult for the West to swallow. The first is the development of a new system of international rules for cyberspace instead of applying existing international law. In China's vision, generally accepted international rules and national codes should be formulated within the framework of the United Nations, and the UN should play a key role in this process. Together with like-minded countries, China advocates a cyber agreement of the Shanghai Cooperation Organisation (SCO), a so-called code of conduct for countries in cyberspace. SCO members want this new agreement to serve as the basis for a new international cyber agreement

China exports its model to other countries through technology and infrastructure as well as international norms

and are therefore actively seeking broader international support for it. The second strategic goal, related to the first, is a reform of the global internet management system that would place the governance of the internet in the hands of the United Nations and its members and transform the Internet Corporation for Assigned Names and Numbers (an NGO under US jurisdiction) into a "truly independent international institution" in which China would actively participate.[14]

Pressure on Rules in Cyberspace

Even if the US and Chinese approaches to cyberspace are similar in generic terms and the stated aim of both superpowers is to cooperate globally for peaceful, secure and open cyberspace, their actions are fundamentally different in terms of content and purpose.[15] As seen by China, the root of the ideological confrontation is, of course, that the norms of behaviour and governance in cyberspace developed in the current system are considered appropriate, above all, to the West.

The collision of interests has been particularly clear during discussions of international law in the UN. The Group of Governmental Experts (GGE) set up by the UN has been the main body that discusses the issues of responsible behaviour of countries in cyberspace and the application of international law.

China has consistently stressed the importance of sovereignty in cyberspace and the link between sovereignty and the protection of critical infrastructure and the supply chain

The current GGE, convened in the autumn of 2018, is the sixth, and China has been actively involved in these discussions since the first in 2004. The GGE is established on the basis of a uniform geographical distribution, and their success so far has lain in the consensus reports that have put in place a general, globally accepted framework for cyber-stability, an integral part of which is the application of international law, and mainly the UN Charter, to state conduct in cyberspace. Unfortunately, in 2017, the members of the group did not reach a consensus, and it is generally believed that this was due to the division of countries into two camps on the issue of international law, including the principal question of the right to respond to foreign cyberattacks by taking countermeasures and exercising the right to self-defence under Article 51 of the UN Charter.[16] This opposition has led to China's current main narrative, which also characterises the ongoing debates on international law.

When the sixth GGE was convened in 2018, a parallel body was set up for the first time, largely under the leadership of China, Russia and like-minded countries: the Open Ended Working Group (OEWG), which deals with similar issues. China has used the latter platform to justify the need to replace the existing rules of international law. China's input to the OEWG stresses that if all countries came to a common understanding on cyberspace norms (including those that have so far been treated as voluntary), this understanding should be interpreted as a legally binding instrument in the future.

Amid ongoing UN discussions, China has consistently stressed the importance of sovereignty in cyberspace and the link between sovereignty and the protection of critical infrastructure and the supply chain. One of China's central messages is that, in order to ensure the peaceful use of cyberspace, any discussion concerning its use for military purposes must be handled with special caution. It rejects the possibility of applying international law on state responsibility to countries' activities in cyberspace and highlights the need for a permanent UN body to ensure long-term planning for cyberspace management.[17] Similar traits are evident in an earlier attempt at UN level to introduce the SCO's Code of Conduct. The purpose of this code was to create a framework that emphasised, among other things, the importance of sovereignty and the need to create a global internet management system.[18]

These are all claims that Western countries find difficult to accept, because their position has been that countries are responsible for their actions in cyberspace in both peacetime and conflict and must adhere to applicable legal restrictions even in the event of a conflict, regardless of the sphere in which the conflict occurs (i.e. physical or cyberspace). Most Western countries emphasise that states must maintain free access to the internet and that their actions in setting up control mechanisms must

always be balanced with the national obligation to ensure human rights. The Freedom Online Coalition, which brings together the governments of 31 countries around the world (including Estonia), argues unequivocally that human rights and cybersecurity are inherently complementary, rather than opposing, phenomena.[19]

Conclusion

There is nothing surprising in the fact that China has begun to convert its economic weight into political influence in the new decade. Nor is it surprising that China proceeds from its own communist ideology and values—including its views on human rights—in doing so. The West needs to think seriously about how we can continue to hold and promote our values in a changing world, namely political and cultural openness, individual human dignity, a liberal market economy, equally in both the physical sphere and cyberspace. There are no quick and simple answers here. Encapsulating and fending off China would be a hasty option, but also a complex or even overwhelming task in economic terms, given today's global supply chains that often depend on China. Cooperation with China must continue in the future, and it is better that it continues without illusions.

References and Notes

[1] Michael Bristow, "China defends internet censorship," BBC News, 8 June 2010.
[2] Michael Bristow, "China defends internet censorship"; Mikk Raud, "China and Cyber: Attitudes, Strategy, Organisation," NATO CCDCOE, 2016.
[3] For years, Google sought a balance between sticking to principles (its 2010 departure from the Chinese market) and adapting (Project Dragonfly, or the Chinese prototype for the Google search engine). Matt Sheehan, "How Google took on China—and lost," *MIT Technology Review*, 8 December 2018; Paul Mozur, "Joining Apple, Amazon's China Cloud Service Bows to Censors," *The New York Times*, 1 August 2017.
[4] Elizabeth C Economy, "The great firewall of China: Xi Jinping's internet shutdown," *The Guardian*, 29 June 2018.
[5] Adrian Shahbaz, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," Freedom House, 2018.
[6] Nicole Kobie, "The complicated truth about China's social credit system," *Wired*, 7 June 2019; Isobel Cockerell, "Inside China's Massive Surveillance Operation," *Wired*, 5 September 2019.
[7] Tian Shaohui (ed.), "Full Text: International Strategy of Cooperation on Cyberspace," Xinhuanet, 1 March 2017.
[8] Tian Shaohui (ed.), "Full Text: International Strategy of Cooperation on Cyberspace," Chapter II.2 (The Principle of Sovereignty).
[9] "Chinese-style 'digital authoritarianism' grows globally: Study," *The Straits Times*, 1 November 2018.
[10] Clayton Cheney, "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism," Council on Foreign Relations, 26 September 2019.
[11] Clayton Cheney, "China's Digital Silk Road."
[12] "Top Contributors: Why China supports ITU," ITU News, 19 September 2018.
[13] The multi-stakeholder governance model involves governments, commercial providers, academia and civil society in the management of the internet.
[14] Tian Shaohui (ed.), "Full Text: International Strategy of Cooperation on Cyberspace," Chapter 4.
[15] Kimberly Hsu and Craig Murray, "China and International Law in Cyberspace," U.S.-China Economic and Security Review Commission, 6 May 2014.
[16] Ann Väljataga, "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," NATO CCDCOE, 2017.
[17] "China's Contribution to the Initial Pre-Draft of OEWG Report," 2020.
[18] Henry Rõigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?," NATO CCDCOE, 2015.
[19] "Human Rights Impact of Cybersecurity Laws, Practices and Policies," Freedom Online Coalition, 2020.

About the Authors

Kadri Kaska
Kadri Kaska heads the Law Branch of the NATO Cooperative Cyber Defence Centre of Excellence. Her field of research is cybersecurity strategy and management in different countries and international law applicable to cyber operations.

Maria Tolppa
Maria Tolppa is a researcher and analyst in the Law Branch of the NATO CCDCOE. Her main area of research is international law applicable to cyber operations.

Disclaimer: The views and opinions expressed in this publication are those of the author and do not necessarily reflect the official position of the International Centre for Defence and Security nor the NATO Cooperative Cyber Defence Centre of Excellence.

ICDS.Tallinn
@ICDS_Tallinn
ICDS-Tallinn
www.icds.ee
EVI.EESTI
@EFPI_EST

International Centre for Defence and Security
Estonian Foreign Policy Institute
Narva mnt. 63/4, 10152 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076