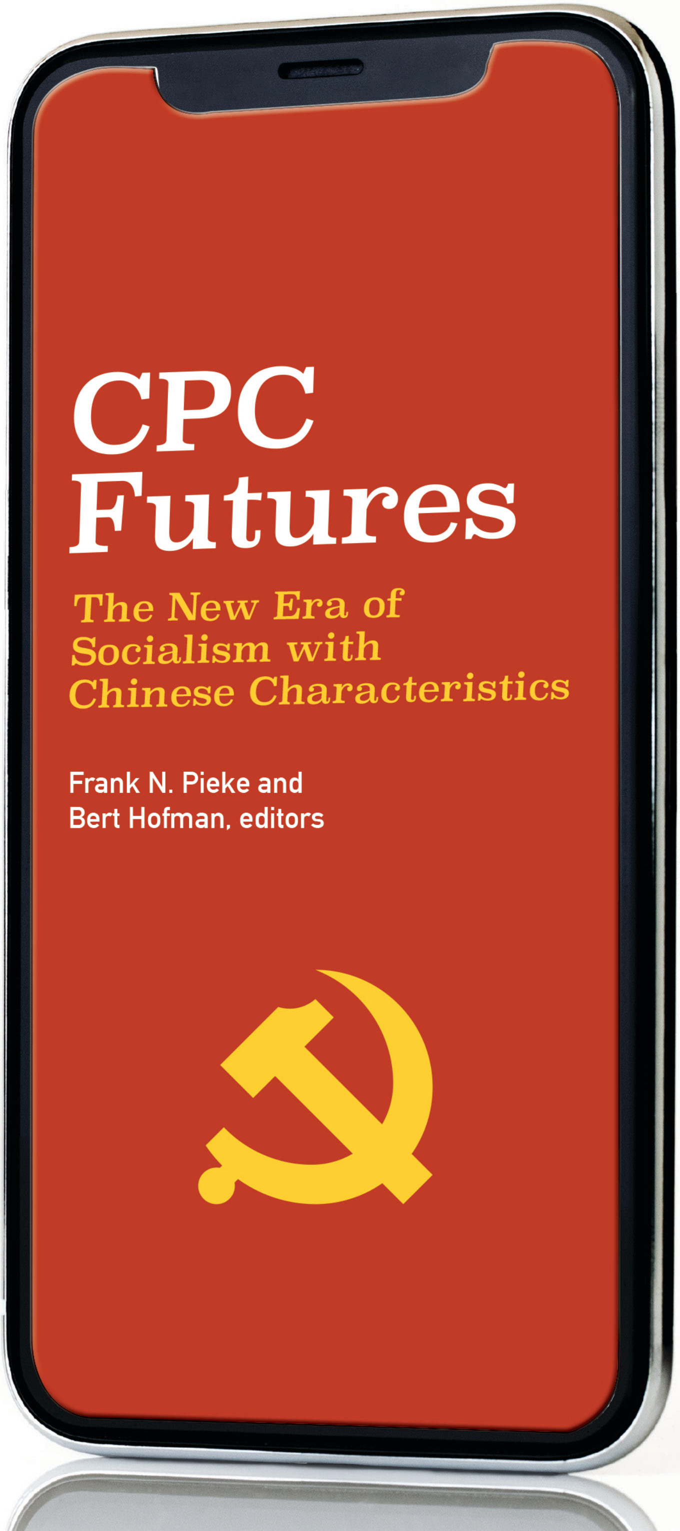

CPC Futures

The New Era of Socialism with Chinese Characteristics

Frank N. Pieke and
Bert Hofman, editors

19

The CPC and Sovereignty in a Digitally Connected World

John Lee

The Party's View of Security in a Digitised World

The goal of China becoming an "advanced information society" was endorsed by the Politburo in 2000. "Informatisation" has continued to guide the state's steerage of China's social and economic development over the past two decades, most recently in the form of a new plan published in late 2021 (Webster et al. 2022). But the Party also recognised the threat to its authority from the internet's enabling of information flows and their potential exploitation by "Western anti-China forces". Edward Snowden's leaks concerning U.S. capabilities in cyberspace and the vulnerabilities of China's digital networks further convinced China's leaders that informatisation could destroy the Party, even while being indispensable to its vision for China and ideological claim to rule. This basic two-sided challenge presented by cyberspace was summarised in 2014 by Xi Jinping: "Without cybersecurity, there is no national security; without informatisation, there is no modernisation" (Xinhua 2014).

Since 2013, the party-state's efforts to harness information and communications technology (ICT) for China's development have been matched by expansion of the policymaking and regulatory apparatus for exerting and securing its authority over cyberspace, conforming with the centralising tendency that has marked Xi's New Era. Accordingly, a Central Commission for Cybersecurity and Informatisation (CCCI) chaired by Xi Jinping now sits atop a new bureaucratic grouping, through which the party-state plans comprehensively to manage activity on China's digital networks (Creemers 2021a).

As the amount of data flowing over digital networks continues to rise exponentially, the party-state is keeping pace by building a comprehensive regulatory system for data transfers and storage. It is seeking to reduce China's vulnerabilities in cyberspace vis-à-vis foreign actors, by building Chinese industry's ability to provide the technologies that constitute digital networks and the cybersecurity capacities to defend them. Asserting the CPC's discourse power on the international stage regarding governance of cyberspace is the foreign policy counterpart to these internal measures to establish China's cyber sovereignty and build China into a cyber superpower that need not fear any external enemy in the CPC's "New Era".

Visibility of Cyberspace

China's well-known system of internet-based information control (including but not limited to the digital border control system known as the Great Firewall) utilising automated filtration and blocking of data transfers, plus extensive manual censorship is now just one element of a growing apparatus that gives authorities access to digital networks. All information networks in China must comply with a tiered security regime (the Multi-Level Protection Scheme) administered by the Public Security Bureau, which has extensive powers to access digital networks and the data stored on them.

China's social credit system, discussed in more detail by Diana Fu and Rui Hou in their chapter in this volume, was conceived to bring a vast scope of activity within a state-regulated environment of trust (or "credit"). The system will increasingly be built on integrated digital databases and data-management tools. The social credit system remains limited and uneven in its scope and application, and is far from completely digitised or rationalised nationwide. But it reflects the general trend of the party-state reimposing control over a society that has grown highly complex over the preceding decades. Regarding corporations, for instance, social credit already centralises legal compliance records for all entities registered in China and automates punishments and rewards based on these records.

Growth in the use of digital networks to deliver both government and private services has simultaneously created a new infrastructure through which the state can exercise control. This was highlighted during the COVID-19 pandemic. Digitised identification technologies and internet-based commercial platforms like WeChat and AliPay were used to monitor and control individual movement (Von Carnap et al. 2020).

The highly intrusive surveillance regime imposed in the Xinjiang region represents the extreme end of the possibilities for societal control that ICT provides to the party-state (Byler 2021). With China moving towards a cashless economy and a state-run digital currency, informatisation is providing the party-state with the means to achieve full transparency of Chinese society by penetrating a cyberspace which is itself increasingly all-pervasive.

Data Governance

China now has in place the world's most comprehensive regulatory regime for data (Creemers 2021b). Built around the three pillars of the Cybersecurity Law, Data Security Law and Personal Information Protection Law—the latter two enacted only in 2021—regulation is being progressively expanded in detail and tailored to different economic sectors. All actors that handle data are required to provide catalogues of data they hold to state agencies, to store certain categories of data inside China and to conduct self-assessments or submit to bureaucratic review before transferring data across China's borders. Internet businesses holding large amounts of personal data are subjected to additional obligations, like submitting to government security reviews before listing on foreign stock exchanges, or ensuring that their recommendation algorithms meet certain requirements.

This still expanding and highly intrusive regime makes no distinction between Chinese and foreign actors. Indeed, the latter are exposed to greater regulatory risk, given the onerous cross-border data transfer controls, the Data Security Law's introduction of a yet unspecified export control system for data, the assertion of extraterritorial jurisdiction over data-related activities that have impacts inside China, and provision for retaliation against foreign government measures concerning the data economy that are perceived to harm Chinese interests. The regime puts constraints on bureaucratic discretion, but these are couched in such broad terms, like "national security" and "public interest", that, unless the constraints are further articulated, it would be hard to predict how much data Chinese authorities may access, or what decisions they make when reviewing data-related activities.

Another element of this new data governance regime is its introduction of state-managed frameworks for data markets, following official endorsement in 2021 of data as an economic factor of production (alongside land, labour and capital). Provision is being made in some sectors and regions for more relaxed controls on cross-border data transfers, reflecting the continued importance of international exchange to China's economic and technological development.

A Chinese Cyber-Industrial Complex

China's 2016 National Cybersecurity Strategy gives equal to weight to countering internal and external threats in cyberspace (Guojia hulianwang xinxi bangongshi [Cyberspace Administration of China] 2016). However, Chinese networks in general appear to remain highly vulnerable to exploitation or attacks by capable foreign actors. One foreign 2021 study judged that China's core cyber defences remained comparatively weak, and that the nation was still in the early stages of building resilience into its critical information infrastructure (International Institute for Strategic Studies 2021).

China has a severe deficit in qualified cybersecurity professionals and a relatively underdeveloped cybersecurity industry. Past failure to prioritise cybersecurity development in line with China's expanding digital economy and infrastructure means it has been playing catchup in this field since the top leadership's attention was focused on it by Edward Snowden's revelations.

Over 2016–17, the CCCI approved a thorough restructuring of China's system for generating a cybersecurity workforce, potentially putting the nation on a path to meet its cybersecurity personnel needs by the late 2020s. China's cybersecurity software sector is growing rapidly and is exploiting new technologies such as artificial intelligence (AI). For the party-state, the goal is a domestic "cyber industrial complex" that provides cybersecurity services of a quality and scale comparable to its U.S. counterpart, and which is considered a prerequisite for China becoming a true cyber superpower.

Being at the leading edge of designing and implementing new technologies should help China close its cybersecurity gap with foreign adversaries. For example, researchers are trying to build "endogenous cybersecurity" into next-generation (6G) telecoms networks, a key element of China's informatisation goals. 6G telecoms and AI are expected to enable intelligent information security systems to better protect military forces during operations (Xie, Xie and Zhang 2020). Such undertakings will directly influence China's prospects in any armed conflict with, for example, the U.S.

ICT Supply Chain Security

Having joined the globalising ICT industry in the 1980s as technological laggards, Chinese firms remain reliant on foreign inputs at many points in their supply chains. In 2016, Xi Jinping identified the greatest hidden danger to China as the foreign powers' control over the core technologies upon which cyberspace is built (Creemers 2018). This judgment has been vindicated over the following years by US export controls targeting selected Chinese firms' dependencies on foreign suppliers. Restricting access to semiconductors by Huawei, for instance, has significantly reduced the Chinese firm's revenue and led to a slowdown in China's nationwide deployment of 5G telecoms infrastructure.

The need to mitigate risks from such politically driven decoupling and to develop secure and controllable ICT systems that minimise vulnerabilities to foreign exploitation have super-charged Chinese import substitution efforts. But China's leaders also recognise that complete independence from foreign suppliers is impossible for the time being, especially in the most complex technologies like semiconductors. The solution, as described by Xi Jinping, is to build structural dependence on China into international supply chains, ensuring that advanced foreign technology providers keep doing business in China, while Chinese firms upgrade their capacity to meet the nation's ICT needs (Xi 2020).

China's centrality in transnational electronics supply chains creates great inertia against foreign efforts to decouple these industries from China, especially given the range of countries and interests involved. This position is being reinforced by China's prominence in developing and commercialising new ICT-enabled technologies, supported by ambitious goals in the 2021–25 14th Five Year Plan (Lee 2021). Meanwhile, Chinese authorities are increasingly mandating import substitution regarding the most severe cybersecurity vulnerabilities.

Normative Dominance Internationally

Since the internet's emergence as a subject of international politics, Chinese diplomacy has used the term "cyber sovereignty" to emphasise the right of national governments to manage cyberspace within their jurisdictions according to their own values and priorities. However, the internet is a globally connected system that originated outside China and has been built largely by private enterprise. Accordingly, on certain issues of global internet governance that bear upon the internet's functioning within China, the party-state has had to accommodate the role of private corporations and some foreign non-government bodies, notably the Internet Corporation for Assigned Names and Numbers (ICANN) (Galloway and He 2014).

Generally however, Beijing's preference has been for matters of global internet governance to be decided in state-centric bodies, such as the International Telecommunications Union, rather than in forums that give more power to corporations or civil society actors. As Chinese firms' technical capabilities have improved, their influence has grown in the international standardisation processes that shape the evolution of telecoms and the internet.

Perceived Chinese state-led efforts to enlist Chinese firms in shaping the design of future ICT infrastructure on an international scale have provoked foreign concerns, sometimes out of proportion to the technical issues involved (Lee 2020). Nonetheless, just as design and governance choices for cyberspace structure power relations within China, so international relations are structured by preferences embedded in global ICT infrastructure. There is not a simple relationship between the CPC's goals and technical choices in internet governance, but the latter do have implications for how China's party-state can exercise power internationally.

China's cyberspace diplomacy has reflected the assertive turn in China's foreign policy under Xi Jinping. In 2014, China began hosting an annual forum for normative discussions about cyberspace, the *World Internet Conference* (WIC), inviting foreign government and ICT industry leaders to China. At the second WIC in 2015, Xi Jinping spoke of "four principles to advance transformation of the global Internet governance system" with respect for cyber sovereignty foremost, and five propositions to build a "community of common destiny" in cyberspace (Xinhua 2015).

China's 2017 *Strategy of International Cooperation in Cyberspace* likewise calls for reform of global internet governance "in the interests of the majority of countries", and positions China as the developing world's champion against western hegemony (China Ministry of Foreign Affairs 2017). China's positions in United Nations forums on cyberspace governance often conflict with those of western countries. Accordingly, minimum levels of cooperation to maintain the internet's basic functionality across borders may be the only realistic prospect for international agreement (Broeders 2015).

Conclusion

By the CPC's own judgment, it cannot stay in power without overcoming the challenges presented by the internet (Zhongyang 2017). The Party now has in place the tools to establish its vision of sovereignty across all key aspects of cyberspace, even if in many areas the necessary conditions remain far from realised. The CPC has achieved this in the context of the profoundly interconnected nature of cyberspace, which facilitates not just reassertion of the Party's control across Chinese society, but also increasingly the extension of its power to the rest of the world. China is arguably one of a few actors capable of shaping the character of international connectivity on a global scale. The party-state's success or failures in the domain of cyberspace will be of profound consequence worldwide and will determine sustainability of its rule over an informationised China.

References

Broeders, Dennis. 2015. *The Public Core of the Internet: An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.

Byler, Darren. 2021. "The Covid Tech That Is Intimately Tied to China's Surveillance State", *MIT Technology Review*, 11 Oct. Available at https://www.technologyreview.com/2021/10/11/1036582/darren-byler-xinjiang-china-uyghur-surveillance/ (accessed 25 July 2022).

China Ministry of Foreign Affairs. 2017. *International Strategy of Cooperation on Cyberspace*, 1 Mar. Available at https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html#:~:text=International%20Strategy%20of%20Cooperation%20on%20Cyberspace%20provides%20a%20comprehensive%20explanation,external%20relations%20on%20that%20front (accessed 8 August 2022).

Creemers, Rogier. 2018. "Xi Jinping's Speech at the National Cybersecurity and Informatization Work Conference", *DigiChina*, 22 Apr. Available at https://digichina.stanford.edu/work/xi-jinpings-speech-at-the-national-cybersecurity-and-informatization-work-conference/ (accessed 8 Aug. 2022).

________. 2021a. *China's Cyber Governance Institutions*. Leiden: Leiden Asia Centre. Available at https://leidenasiacentre.nl/report-chinas-cyber-governance-institutions/ (accessed 9 June 2022).

________. 2021b. "China's Emerging Data Protection Framework", SSRN, 14 Dec. Available at https://ssrn.com/abstract=3964684 (accessed 9 June 2022).

Galloway, Tristan and He Baogang. 2014. "China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF", *China: An International Journal* 12, 3: 72–93. Available at muse.jhu.edu/article/563560 (accessed 8 Aug. 2022).

Guojia hulianwang xinxi bangongshi 国家互联网信息办公室 [Cyberspace Administration of China]. 2016. *Zhongguo wangluo kongjian anquan zhan lüe* 国家网络空间安全战略 [National Cybersecurity Strategy], 27 Dec. Available at http://www.cac.gov.cn/2016-12/27/c_1120195926.htm (accessed 8 August 2022).

International Institute for Strategic Studies [IISS]. 2021. *Cyber Capabilities and National Power: A Net Assessment.* London: IISS. Available at https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (accessed 8 Aug. 2022).

Lee, John. 2020. "Will China Reinvent the Internet?." *The China Story*, 28 Apr. Available at https://www.thechinastory.org/will-china-reinvent-the-internet/ (accessed 8 August 2022).

________. 2021. *The Internet of Things: China's Rise and Australia's Choices*. Sydney: Lowy Institute. Available at https://www.lowyinstitute.org/publications/the-internet-of-things-chinas-rise-and-australias-choices (accessed 9 June 2022).

Von Carnap, Kai, Katja Drinhausen and Kristin Shi-Kupfer. *Tracing. Testing. Tweaking: Approaches to Data-driven Covid-19 Management in China*. Berlin: Mercator Institute for China Studies. Available at https://merics.org/en/report/tracing-testing-tweaking (accessed 9 June 2022).

Webster, Graham et al. 2022. "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021". *DigiChina*, 24 Jan. Available at https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/ (accessed 8 Aug. 2022).

Xi Jinping 习近平. 2020. "Guojia zhong-changqi jingji shehui fazhan zhanlüe ruogan zhongda wenti" 国家中长期经济社会发展战略若干重大问题 [Several major issues in the national medium- and long-term economic and social development strategy], 31 Oct. Available at http://www.qstheory.cn/dukan/qs/2020-10/31/c_1126680390.htm (accessed 8 Aug. 2022).

Xie Ruikun 谢瑞鹍, Xie Ruipeng 谢瑞鹏 and Zhang Qingliang 张清亮. 2020. "Ruguo 6G yunyongyu weilai zuozhan" 如果6G运用于未来作战 [What if 6G were used in future operations], *Zhongguo junwang* 中国军网 [China Military Network], 14 Apr. Available at http://www.81.cn/gfbmap/content/2020-04/14/content_258839.htm (accessed 8 Aug. 2022).

Xinhua 新华. 2014. "Xi Jinping: ba woguo cong wangluo daguo jianshe chengwei wangluo qiangguo" 习近平: 把我国从网络大国建设成为网络强国 [Xi Jinping: Build our country from a big network country to a network superpower], 27 Feb. Available at http://www.xinhuanet.com/politics/2014-02/27/c_119538788.htm (accessed 8 August 2022).

________. 2015. "Xi Jinping jiu gongtong goujian wangluo kongjian mingyun gongtongti tichu 5 dian zhuzhang" 习近平就共同构建网络空间命运共同体提出5点主张 [Xi Jinping Puts Forward "Five Propositions" for Building a Community of Common Destiny in Cyberspace], 16 Dec. Available at http://www.xinhuanet.com//world/2015-12/16/c_128536396.htm (accessed 8 August 2022).

Zhongyang wangxin banli lunxue xuexi zongxinzu 中央网信办理论学习中心组 [Central Network Information Office Theory Learning Center Group]. 2017. "Shenru Guanche Xi Jinping zongshuji wangluo qiangguo zhanlüe sixiang tashi tuijin wangluo anquan he xinxihua gongzuo" 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 [Deepening the implementation of General-Secretary Xi Jinping's strategic thinking on building China into a cyber superpower: steadily advancing cybersecurity and informatisation work], 15 Aug. Available at http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm (accessed 25 July 2022).

DOI: https://doi.org/10.56159/eai.52060.20