NOTES
DE L'IFRI

ASIE.VISIONS, No. 129

JULY
2022

Cyberspace Governance in China

Evolution, Features and Future Trends

Center for Asian Studies

John LEE

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0573-2

How to quote this publication:
John Lee, "Cyberspace Governance in China: Evolution, Features and Future Trends", *Asie.Visions*, No. 129, Ifri, July 2022.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

John Lee is director of the consultancy East West Futures. He is also a researcher at the Leiden Asia Center and a consultant for the International Institute of Strategic Studies. John's research focuses on China and digital technology, in particular China's cyberspace governance regime, the semiconductor industry and future telecommunications networks. Previously he was a senior analyst at the Mercator Institute for China Studies and worked at the Australian Department of Foreign Affairs and Trade and Department of Defence. John holds a Master of Laws (International Law) from the Australian National University and a Master of Arts (War Studies) from King's College London. To contact the author, visit his website: eastwestfutures.com.

Executive Summary

The growing pervasiveness of cyberspace has made its governance a key factor in international trade and politics. Even as China's political relations with most of the world's technologically advanced states have worsened, Beijing has put in place the world's most comprehensive regulatory and administrative system for governing cyberspace. Increasingly onerous compliance challenges for actors using Chinese cyberspace, and China's recent crackdown on internet technology firms have focused foreign attention on the Chinese Party-state's goals for this critical domain.

To understand these goals, it is not sufficient to look at recent events and contemporary pressures. China's cyberspace governance regime is the result of a decades-long development process, over which the Party-state has responded to the global evolution of cyberspace and defined its interests against changing conditions. The emergent nature of cyberspace has created significant governance challenges even for the most technologically advanced nations. China entered this domain from a disadvantageous technological position, in the course of rapid development and relative political liberalization. Accordingly, China's Party-state relatively early recognized cyberspace governance as an existential issue. Quoting the Chinese Communist Party's journal of record, 'if our Party cannot overcome the obstacles presented by the internet, it cannot maintain its long-term hold on power.'[1]

This report summarizes the development of the Party-state's engagement with the internet and the global digital technology industry, and the evolution of its policies towards managing cyberspace as an integrated whole. It then discusses the main actors and their roles in the 'noodle bowl' of institutions involved in governing Chinese cyberspace. Although still characterized in many respects by bureaucratic overlap and unclear definitions, this institutional system has now stabilized enough for its main aspects to be described. The same is true of China's evolving regulation for cyberspace, the most important elements of which are described in the report's next section, in particular the increasingly onerous rules governing data handling and cross-border data transfers.

In conclusion, China's system for cyberspace governance and its future development is discussed in international context. For foreign governments as well as private actors, learning to engage with this system is an

1. 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, *Quishi*, September 15, 2017, available at: www.qstheory.cn.

unavoidable task that will only become more complex and risk-laden, as the Party-state's goals become more ambitious and political relations with Western countries show few signs of improving. Yet China's unique model may also provide constructive lessons for other nations, being shaped by many of the same challenges that cyberspace presents to societies worldwide.

Table of Contents

Introduction

As ever more activity is conducted over digital networks, cyberspace governance has emerged as a key factor in international trade and politics. States are expanding their control over activity in cyberspace, while political tensions are affecting the cross-border flows of goods and information upon which globalization has been built. The biggest international fault lines are around China, which has increasingly antagonistic political relations with Western countries, and has put in place the world's most comprehensive regulatory and administrative system for governing cyberspace.

Much attention has been given to China's recent promulgation of sweeping laws concerning data governance and regulatory crackdown on its internet technology companies. These developments are compounding the compliance challenges and risks for foreign actors trying to do business in or with China, even as the nation looms ever larger in emerging technologies and digital markets worldwide. Explanations for this behavior by Chinese authorities are being sought in the country's current political or economic conditions, in the hope that changes in these circumstances would lead the Chinese government to revert to a more *laissez-faire* attitude towards the digital economy.

Yet, to look solely to the current context in China for answers misses the longer-term trendlines. China's cyberspace governance regime is the product of decades of evolution, and of deep-rooted judgments by Chinese leaders about the relationship between cyberspace and national priorities. New elements like China's Data Security Law or cybersecurity reviews of internet technology firms should not be viewed in isolation, but as part of a larger and still-evolving framework. Rather than focusing on China's crackdown on internet technology firms and extrapolating conclusions from this about the future, foreign observers should seek instead to understand how the Chinese Party-state views cyberspace, and how long-term policy goals have shaped its cyberspace governance system.

While this system is now comprehensive, it has many design flaws, leaves Chinese officials wide discretion for decision making, and still requires much articulation in detail. In many respects, it is not yet possible to describe clear spheres of bureaucratic authority or specific compliance obligations. But this system will increasingly impose itself on every aspect of foreign exchanges with China, as the use of cyberspace for human activity becomes ever more pervasive worldwide.

This report summarizes how the Chinese Party-state's cyberspace policy has evolved over the decades and reached its present form. The main elements of China's cyberspace governance system – institutional actors, laws and regulations – are then described, looking in particular at the implications for cross-border data transfers. The report concludes with a look at implications for China's handling of its international connections in cyberspace, and lessons for European policymakers in the context of the EU's own expanding regime for cyberspace governance.

The Evolution of Cyberspace Policy and Governance in China: Prioritizing both Development and Security

The Early Years: Use of Foreign Technology, but with Chinese Characteristics

From the outset, the Internet's expansion within China and its connections with the outside world were designed to enable state visibility and control over the entire network nationwide. The network was physically structured to facilitate filtering of cross-border traffic, using equipment and software provided by US companies (notably Cisco). The same methods employed by private corporations elsewhere in the world to inspect and control digital data transfers were employed at national scale to monitor and censor China's connections with foreign networks. This was reinforced by an internal censorship system that devolves responsibility onto firms and institutions providing internet-based services at the consumer level, and has historically relied heavily on manual censorship work, with state authorities taking a selective approach to intervention in politically prioritized cases.[2]

The Chinese internet should thus be thought of not as a separate internet, but as a branch of the global internet that is controlled at the international border, comparable to how states' immigration and customs authorities control passage across borders in the physical world.[3] Although efficiency penalties are imposed by the technical requirements of content filtering, Chinese networks have historically been interoperable with foreign ones because they are built on essentially the same technology as anywhere else in the world. Before the 2000s, this technology was produced almost entirely by firms from the developed economies and especially from the US.

2. J. Griffiths, *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*, London: Zed Books, 2019, chapter 2.
3. M. Mueller, *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*, Cambridge: Polity, 2017.

Even as they embedded mechanisms of control over their population's access to cyberspace, Chinese authorities also promoted the rapid expansion of internet infrastructure from the late 1990s. But beyond political censorship, state actors initially gave little attention to regulating this emerging Chinese cyberspace, or to developing products and services to use it.[4] This vacuum was filled by private entrepreneurs, who exploited economic liberalization and the imperative for local governments to achieve growth and development. Liberalization of international travel allowed Chinese nationals to go to the US for formal education and work experience in the Information and Communication Technology (ICT) sector, giving them skills and ideas which they brought home to monetize with China's growing online population.[5]

Whether or not there was deliberate state policy to keep out foreign market leaders to foster the growth of domestic equivalents, the censorship regime's effects and political constraints hampered US internet platform giants from establishing themselves in Chinese cyberspace. Foreign firms also often failed to adapt to local conditions or to take the steps necessary to succeed in the brutal competition of China's online markets. But the operations in China of US companies like Microsoft and Apple helped foster the development of Chinese ICT firms in software and hardware sectors. For example, Apple's manufacturing operations in China have stimulated development of a globally competitive supplier network of Chinese firms and the upskilling of the Chinese labor force.

Informatization: Building China's Capabilities in Digital Technologies

The policy context for all this activity was guidance from the top of China's political system that the expanded application of ICT was a national policy priority. As early as 1992, developing the information economy was identified as an important policy objective. The priority placed by China's top leaders on joining the global ICT-enabled economy was symbolized by meetings in the mid-1990s between Microsoft's Bill Gates and the CCP's General Secretary and President of China, Jiang Zemin.[6]

The state's rubric for this expansion of ICT's use is 'informatization' (信息化). In 2000, the Politburo resolved that it would be a first-rank policy priority to develop China into an 'information society', with transformative

4. T. M. Cheung, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities", *Journal of Cyber Policy*, Vol. 3, No. 3, 2018, pp. 314-315.
5. J. Lee, "The New Chinese Diaspora", *The Interpreter*, Lowy Institute, March 31, 2017, available at: www.lowyinstitute.org.
6. G. Austin, *Cyber Policy in China*, Cambridge: Polity, 2014, pp. 34-35.

effects for economic productivity.[7] A fifteen-year National Informatization Development Strategy (NIDS) was issued in 2006 by the State Council, the highest organ in China's executive government, and ICT development has been a consistent theme in national policy statements over the last two decades. Notably, in 2015 the State Council promulgated an 'Internet Plus' document that promoted 'deep integration' of the internet with all aspects of China's economy and society, as well as the 'Made in China 2025' guidelines for helping Chinese industry to reach the technological frontier across a range of sectors, with ICT-related industries featuring prominently.

Underpinning this long-term commitment is the CCP's process of theoretical justification for its policies, which has long identified 'informatization' as a world-historical trend that China must keep pace with if it is to modernize and maintain itself against hostile foreign powers. The re-politicization and increase in CCP control throughout Chinese society since Xi Jinping's accession to leadership in 2012 is inherently in tension with an 'information society' as understood in liberal democracies. But the reiteration under Xi's rule of the 'informatization' goal shows that the CCP's leaders remain confident in their capacity to reconcile this basic contradiction: to 'nail Jell-O to the wall', using Bill Clinton's metaphor for the challenge of policing social behavior in cyberspace.

This broad policy framework has been matched by tangible measures, albeit with varying degrees of success, intended to stimulate the development and deployment in China of ICT technologies and infrastructure. For example, from the mid-2000s the national government began promoting development of 'Internet of Things' (IoT) technologies, developing R&D clusters in particular locations with long-term support from local government and using these to support technical progress by Chinese industry champions such as Huawei.[8] In recent years the state has pushed rapid development of 'new-type infrastructure' to enhance digital connectivity on a national scale, notably a world-leading pace of equipment deployment for fifth-generation (5G) telecoms networks.[9]

Securitization: Rebalancing the Development of Chinese Cyberspace

One result of the initial regulatory vacuum in Chinese cyberspace was that the growth of ICT infrastructure and related industries far outstripped the development of concomitant cybersecurity capabilities. The state's focus on political censorship long absorbed much of the resources available for

7. *Ibid*, p. 49.
8. J. Lee, "The Connection of Everything: China and the Internet of Things", *China Monitor*, MERICS, June 24, 2021, available at: merics.org.
9. C. Meinhardt, "China Bets on 'New Infrastructure' to Pull the Economy Out of Post-Covid Doldrums?", MERICS, June 4, 2020, available at: merics.org.

protective measures in cyberspace, and the censorship machinery itself created sources of vulnerability.[10] The 2006 NIDS identified risks in the excessive reliance on technology imports and the lack of investment in developing domestic capabilities, and followed up an earlier directive for establishment of a multi-level national information security system. By the late 2010s, China had developed a diversified cybersecurity industry, with Chinese firms of varying pedigree providing services to customers at all levels throughout Chinese cyberspace.[11]

Xi Jinping took up national leadership in the same year that Edward Snowden's disclosures revealed extensive compromise of Chinese networks by the US government, including through the cooptation of leading American private sector ICT providers. In response, China's new leadership took steps to address the fragmentation of responsibility for cybersecurity among state agencies, elevate cybersecurity to a policy goal of equal status with 'informatization', and impose top-level centralized oversight. The key step was establishment of the Central Commission for Cybersecurity and Informatization (CCCI) in early 2014, chaired by Xi Jinping and bringing together senior representatives from across China's bureaucracy, academia and military. The CCCI's executive office is the Cyberspace Administration of China (CAC), which in addition to providing the CCCI with administrative support has progressively accumulated a range of responsibilities, detailed in the section below.

The Snowden revelations spurred Chinese authorities to double down on import substitution in ICT procurement and development of domestic capacity in 'core technologies', such as computer processors and software operating systems. The national leadership has also recognized China's severe deficit in cybersecurity professionals and taken steps to promote training of skilled labor in this field, and a holistic approach to cybersecurity based upon international best practice.[12] But China is starting from a low base, and the growth in this labor pool remains far from equipping the nation to meet basic cybersecurity requirements across large swathes of its digital infrastructure.

One US commentator assessed in 2015 that China's technical cybersecurity environment remains typified by 'uneven [cyber]industrial development, fragmented cyber defenses, uneven cyber operator tradecraft, and the market dominance of Western information technology arms'.[13]

10. R. Clayton, S. J. Murdoch, and R. N. M. Watson, "Ignoring the Great Firewall of China", in: G. Danezis and P. Golle (eds.), *Privacy Enhancing Technologies*: *Lecture Notes in Computer Science*, Vol. 4258, Conference Paper, 2006, available at: link.springer.com.
11. T. M. Cheung, "The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities," *op. cit.*, pp. 306-326, p. 315.
12. G. Austin, *Cybersecurity in China: The Next Wave*, New York: Springer, 2018, pp. 6-35.
13. J. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security*, Vol. 39, No. 3, Winter 2014/2015, pp. 7-47, p. 27.

A comparative study of national cyber capabilities published in 2021 judged that China's core cyber defenses remained relatively weak, and that the country is still in the early stages of building resilience into its critical information infrastructure.[14] These insecurities have only been exacerbated by US targeting of China's foreign dependencies in essential ICT technologies, notably semiconductor manufacturing, in a context of worsening relations. A sense of deep vulnerability shapes the policy and regulatory juggernaut now being directed by Chinese authorities at gaining visibility and control over China's cyberspace environment, even as they seek to exploit it for national development goals.

This sense of vulnerability both to foreign actors with superior capabilities for computer network exploitation (CNE) and cyber warfare, and to domestic political dissent propagating over the internet, was reflected in the National Cybersecurity Strategy (NCSS) issued by the CAC in 2016.[15] The NCSS addresses 'two great situations' (domestic and foreign threats) and frames cybersecurity as a comprehensive social-technical practice. At the same time, the strategy enshrines Xi Jinping's emphasis on the use of cyberspace to propel national development as a coequal and intertwined value with cybersecurity.[16]

In 2016, China also enacted its national Cybersecurity Law (CSL), introducing framework obligations that have been subsequently articulated through subordinate regulation and policy practice. Through the late 2010s, the national government released drafts of new laws and policies concerning cyberspace for public consultation, developed with the support of China's system of state-linked technical committees and academic institutions, and reflecting learnings from foreign models such as the European Union's General Data Protection Regulation (GDPR). In parallel, China's digital economy expanded dramatically, with the nation's massive and growing online population conducting a widening range of activities through online 'super-apps', controlled by private Chinese firms, two of which (Alibaba and Tencent) joined the world's biggest companies by market valuation.

Equitable Development, Self-reliance, and the Party-state's Evolving Goals for Cyberspace

The CCP Congress of 2017 marked a political re-orientation away from breakneck economic growth towards a more sustainable and socially

14. *Cyber Capabilities and National Power: A Net Assessment*, Institute for International Strategic Studies, June 28, 2021, available at: www.iiss.org.
15.《国家网络空间安全战略》全文, Cyberspace Administration of China, December 27, 2016, available at: www.cac.gov.cn.
16. G. Austin, *Cybersecurity in China: The Next Wave*, *op. cit.*, p. 7.

equitable development paradigm.[17] Policy statements have also increasingly emphasized integration of the digital with the real economy, and re-orientation of resources away from internet platform services and accumulation of monopolistic power by firms in this sector towards building 'core technologies' such as semiconductors. This focus on ensuring that development of the digital economy serves the real economy and the interests of society as a whole is the key context for the state's crackdown on China's internet technology businesses during 2021, which was in fact quite limited in scope and measures.[18] Simultaneously, the digital economy has been prioritized to compensate for China's slowing economic growth, given its relatively fast expansion, which in 2019 was estimated at roughly twice the nation's GDP growth rate.[19]

In 2020, official Chinese rhetoric introduced the concept of 'dual circulation' as a strategic goal for China's economic development. In Xi Jinping's words, the objective is for domestically contained activity to gradually assume a dominant role in China's economy.[20] This policy evolution paralleled the introduction of expanded US export controls targeting Huawei, which severely undermined the Chinese firm's ability to produce cutting-edge products, and so highlighted the vulnerabilities implied by continued dependence on foreign providers of 'core technologies.' Chinese authorities are boosting efforts to help domestic firms close the gap with global leaders in the semiconductor sector, and private ICT firms are increasingly taking steps towards import substitution.[21] Raising national 'self-reliance' is now consistently emphasized in official discourse on technology policy.

However, China's senior leaders also clearly understand that the nation's capability gaps in many aspects of ICT will persist for years to come, and that China needs cooperative international links in cyberspace to achieve the state's digital development goals. In an October 2021 speech to the Politburo, Xi Jinping directed that China should 'vigorously participate in international cooperation on the digital economy'.[22] In January 2022, China's Minister of Industry and Information Technology published a commentary in the People's Daily stating that state policies will promote

17. K. Rudd, *The Avoidable War: The Dangers of a Catastrophic Conflict between the US and Xi Jinping's China*, New York: PublicAffairs, 2022.
18. R. H. Huang and J. Henderson, "Is There a Method Behind China's Tech Crackdown Madness?", MacroPolo, October 21, 2021, available at: macropolo.org; C. Che and J. Goldkorn, "China's 'Big Tech Crackdown': A Guide", *SupChina*, August 2, 2021, available at:supchina.com.
19. *White Paper on China's Digital Economy Development*, China Academy of Information and Communications Technology (CAICT), 2020, available at: www.caict.ac.cn (PDF).
20. F. Tang, "What Is China's Dual Circulation Economic Strategy and Why Is It Important?", *South China Morning Post*, November 19, 2020, available at: www.scmp.com.
21. J. Lee and J. P. Kleinhans, "Mapping China's Semiconductor Ecosystem in Global Context: Strategic Dimensions and Conclusions", *MERICS Report*, June 30, 2021, available at: merics.org.
22. "Translation: Xi Jinping's Speech to the Politburo Study Session on the Digital Economy – Oct. 2021", DigiChina, Stanford University, January 28, 2022, available at: digichina.stanford.edu.

'all-round opening-up in the manufacturing sector', foreign investment in mid and high-tier manufacturing, and international cooperation on industrial and supply chains.[23]

Through 2021 and early 2022, China adopted a Data Security Law (DSL), Personal Information Protection Law (PIPL) and various regulations concerning commercial activities in cyberspace, for example governing recommendation algorithms for internet-based services.[24] This reflected the general tightening of control over China's internet platform giants and their 'disorderly expansion of capital', with state agencies increasingly equipped with means to supervise and discipline these companies' activities. These companies, most notably Alibaba, were publicly reprimanded and subjected to fines, forced restructuring and other administrative penalties. 2021 was likely viewed by Chinese authorities as the opportune year, between the initial COVID pandemic year of 2020 and the 20th CCP Congress in 2022, at which Xi Jinping is expected to be endorsed for a new leadership term, to take such necessary regulatory action while minimizing the associated economic and political repercussions.[25]

In the last week of 2021, the national government adopted another spate of cyberspace-related regulations and policies, most importantly the 14th Five-Year Plan for National Informatization (FYPNI). Issued by the CCCI, this document sets strategic guidance 'for informatization work in all localities and all department' out to 2025.[26] The FYPNI designates data as a 'factor of production,' elevated to equal status with land, labor and capital in the Marxist theoretical framework for policy in China. Consistent with 'dual circulation', the FYPNI promotes development of a diversified and mutually catalyzing 'ecology' of actors in China's digital economy. It sets out ten policy priorities that encompass infrastructure building, exploiting data as a productive factor, digitizing government services, and strengthening international cooperation in management of global cyberspace.

Ultimately, China arrived at its current cyberspace governance system not through *ex ante* vision and a well-defined design process, but through a drawn out, messy and iterative evolution. Yet, this process of development has produced not just clear policy guidelines for state intervention in cyberspace, but also a comprehensive institutional system and regulatory framework for managing it. The following section looks at the latter two elements in more detail.

23. Y. Q. Xiao, 充分发挥工业的"压舱石"作用（经济形势理性看, People's Daily, January 20, 2022, available at: paper.people.com.cn.
24. "Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022", DigiChina, Stanford University, January 10, 2022, available at: digichina.stanford.edu.
25. R. H. Huang and J. Henderson, "Is There a Method Behind China's Tech Crackdown Madness?", *op. cit.*
26. "Translation: 14th Five-Year Plan for National Informatization – Dec. 2021", DigiChina, Stanford University, January 24, 2022, available at: digichina.stanford.edu.

Key Institutional Actors in China's Cyberspace Governance 'Noodle Bowl'

China has effectively created a new "*xitong*", or functional grouping of state agencies for coordinating a given policy field, to implement cyberspace governance.[27] Like the accompanying regulatory framework described below, this system resembles less a Lego set than a noodle bowl: the precise relationship between actors and the extent of their authority are not clearly defined, and there are significant bureaucratic overlaps and apparent redundancies. In its current form, this noodle bowl of institutions and regulations arguably owes as much to bureaucratic inertia, infighting, and resulting compromises as to purposeful *ex ante* design. But the most important agencies and their key competencies can be described, reflecting stabilization of the Party-state's priorities for cyberspace and its management approach, following the long evolutionary process outlined above.[28]

Central Commission for Cybersecurity and Informatization (CCCI)

The CCCI**,** nominally chaired by Xi Jinping and co-chaired by other members of the Politburo Standing Committee, supervises the entire cyberspace *xitong*. The extent to which this body engages with detailed policy issues is opaque, but its existence dampens incentives to pursue bureaucratic turf wars by bringing them within the top leadership's view, and it provides a forum for resolving such disputes in an authoritative manner. The body's nomenclature sends an unambiguous message that security is a coequal value and indivisible with 'informatization'. As Xi declared at the CCCI's inaugural meeting in 2014: 'cybersecurity and informatization are two wheels of a single drive… there is no national security without cybersecurity, and no modernization without informatization'.[29]

---

27. R. Creemers, "China's Cyber Governance Institutions", Leiden Asia Centre, January 2021, available at: leidenasiacentre.nl; T. Saich, *Governance and Politics of China*, New York: Palgrave Macmillan, 2010, pp. 122-123.
28. *Ibid*.
29. 习近平:把我国从网络大国建设成为网络强国, *Xinhua*, February 27, 2014, available at: www.xinhuanet.com.

Cyberspace Administration of China (CAC)

As the CCCI's supporting office, the CAC – which evolved from a body that was originally tasked with online censorship – has been well positioned to acquire a range of competencies involving supervision of state and quasi-state entities, policy coordination and regulation. The CAC has no enumerated list of responsibilities, but its position at the top of the cyberspace *xitong* has led to progressive extension of its activities. In regulatory measures the CAC acts in concert with line bureaucracies, but unlike the latter it is not subject to accountability mechanisms under Chinese administrative law, such as enforceable remedies or the obligation to publish reasons for decisions. Illustrating its breadth of competencies, the CAC now *inter alia* oversees the entity that manages the internet's addressing system (DNS) within China, has lead responsibility for implementing the PIPL through development of subordinate regulation and standards, and initiates cybersecurity reviews into critical information infrastructure (CII) operators and internet platform providers (IPPs).[30]

CII is incompletely defined in extant legislation and regulation, but includes *inter alia* 'important network infrastructure, information systems etcetera in important industries and sectors such as public telecommunications and information services, energy, transportation… where their destruction, loss of functionality or data leakage may gravely harm national security…'.[31] IPPs provide services comparable to US companies like Google, Amazon and Uber. In China, these range from relatively small scale providers to vast horizontally-integrated businesses like Alibaba and Tencent, with the latter being subject to distinct regulatory obligations, as noted below.

The CAC is in charge of regulating the export of personal information outside China's borders and coordinating 'formulation of concrete personal information protection rules and standards.'[32] It is also overseeing development of cross-border data transfer regimes specific to

30. R. Creemers, "China's Cyber Governance Institutions", *op. cit.*, p. 7; "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", DigiChina, Stanford University, September 7, 2021, available at: digichina.stanford.edu; 网络安全审查办法-中共中央网络安全和信息化委员会办公室, Cyberspace Administration of China, January 2022, available at: www.cac.gov.cn.
31. "Translation: Critical Information Infrastructure Security Protection Regulations (Effective Sept. 1, 2021)", DigiChina, Stanford university, August 18, 2021, Article A2, available at: digichina.stanford.edu.
32. PIPL, Articles 38 and 62.

pilot zones around China designated for the development of innovative trade in services.[33]

China's new DSL makes the CAC 'responsible for comprehensive coordination of network data security and related regulatory work', and for formulating security measures to govern exports of 'important data' outside China in cooperation with other agencies.[34] Having also received primary responsibility for implementing the new Five-Year Plan for National Informatization, the CAC seems to be cementing its role as China's lead coordinating agency for cyberspace policy. This probably owes much to its 'dual-badged' nature,[35] being simultaneously an organ of China's executive government and of the CCP. The CCCI's upgrade to Central Commission status in 2018 placed it directly under the CCP's Central Committee.[36] This proximity to China's top-level leaders means that the CAC (as the CCCI's executive office) is likely favored by them as an implementation vehicle for policy, and more responsive to their views than to technocratic considerations.

Even as the CAC has accumulated technocratic functions, all its directors have concurrently been vice-directors of the CCP's Central Propaganda Department, underscoring the centrality that ideological work continues to hold in Chinese leaders' conception of cybersecurity. By 2014, the CAC had usurped the old propaganda bureaucracy's role regarding online communications.[37] This reflects the CCP's view of the internet as 'the main battleground and most-forward position' of ideological warfare against foreign powers and domestic dissent.[38] Fears of the internet's subversive potential have been reinforced by US commitment to promoting 'internet freedom' as a foreign policy principle, and the role of social media in popular revolutions across Arab and ex-Soviet countries. Disseminating 'positive energy' (ideologically correct thinking) throughout Chinese cyberspace is a ubiquitous theme, appearing for instance in the new regulations for recommendation algorithms.[39]

33. "Sino-German Cooperation on Industrie 4.0: Policy Update on Innovative Development of Trade in Services in Pilot Areas", *Plattform Industrie 4.0*, Federal Ministry for Economic Affairs and Climate Action, September 1, 2020, available at: www.plattform-i40.de.
34. DSL, Articles 6 and 31.
35. 'One body, two plaques' (一个机构两块牌子)
36. 国务院关于机构设置的通知, State Council, People's Republic of China, March 24, 2018, available at: www.gov.cn.
37. R. Creemers, "China's Cyber Governance Institutions", *op. cit.*, p. 7.
38. R. W. Zhuang, "Scientifically Understanding the Laws of Internet Communication, Strive to Raise the Level of Use and Governance of the Internet", Qiushi, September 16, 2018, available at: www.qstheory.cn.
39. "Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022", DigiChina, Stanford University, January 10, 2022, available at: digichina.stanford.edu, Article 6.

Ministry for Industry and Information Technology (MIIT)

While the MIIT has lost various functions to the CAC, it retains influence over extensive elements of Chinese cyberspace, for example construction of telecoms networks and related security measures, and regulatory authority over the DNS (global internet addressing system).[40] This authority over digital infrastructure puts the MIIT in the driver's seat for determining how much of the cyberspace 'terrain' is designed in practice, notably through development of the Internet of Things, including related technical standardization.[41] Together with China's Public Security Bureaus, the MIIT jointly issues catalogues of ICT products that are subject to security certification or inspection by state authorities under the CSL. The MIIT is responsible for developing dedicated internet data channels in innovative services trade pilot zones, where cross-border data transfer regimes are likely to be less restrictive than elsewhere.[42]

China Academy for Information and Communication Technologies (CAICT)

The MIIT's affiliated research organization, the CAICT, has a prominent role in shaping applications of technology in cyberspace, including through international collaborations. For example, the CAICT has been working with China's Artificial Intelligence Industry Alliance on testing and certification of AI systems, and it recently began issuing 'trustworthy AI' certifications for facial recognition software.[43] The CAICT is the Chinese lead in the Sino-German *Industrie 4.0* partnership for developing intelligent manufacturing, and it has led development within China of a digital addressing system for the industrial internet.[44]

National Information Security Standardization Technical Committee (TC260)

The CAICT is one of several technical bodies that concentrate the expertise required to articulate policy, regulations and standards for Chinese cyberspace, and which are linked to the state apparatus. Another

40. R. Creemers, "China's Cyber Governance Institutions", *op. cit.*, p. 13-14.
41. J. Lee, "The Connection of Everything: China and the Internet of Things", *op. cit.*
42. Federal Ministry for Economic Affairs and Climate Action, 2021, *op. cit.*
43. J. Lee, E. Zhang and R. Creemers, "China's Standardisation System – Trends, Implications and Case Studies in Emerging Technologies", Leiden Asia Centre, April 2022, available at: leidenasiacentre.nl.
44. J. Lee, "The Connection of Everything: China and the Internet of Things", *op. cit.*

is TC260, which is headed by the CAC's deputy director and brings together senior leaders from agencies including the MIIT, the Ministry of Public Security, the State Cryptography Administration and the State Administration of Market Regulation (SAMR). Under China's highly structured standards system, official standards influence the implementation and regulation of technology in a variety of ways.[45] Concerning data regulation, for example, TC260 has published draft standards for guidelines on identifying 'important data' (a key term that appears in the CSL and DSL without elaboration) and for data classification generally.[46]

Ministry of Public Security (MPS)

Another key actor is the MPS, which commands China's police forces. The MPS oversees China's multi-level protection system, with antecedents dating back to 1994, which is a national grading system for information security that subjects all digital networks to security requirements that increase in tiers of sensitivity.[47] To ensure compliance by actors providing internet-related services, the MPS has powers to physically or remotely access digital systems, take copies of data and demand explanation of how systems are configured.[48]

Despite the CAC's steady accrual of competencies, the MPS has secured its role as the lead agency for hands-on implementation of cybersecurity in China, including for CII specifically.[49] Regarding data governance, the DSL recognizes the MPS' role by providing that 'public security authorities… undertake data security regulatory duties within their scope of their respective duties.'[50] The MPS leads periodic campaigns to enforce the cyberspace regulatory regime. In 2019 the MPS, CAC, MIIT and SAMR set up an 'App Governance Working Group' comprising TC260

45. T. Rühlig, "The Shape of Things to Come: The Race to Control Technical Standardization", European Chamber of Commerce in China, December 2, 2021, available at: www.europeanchamber.com.cn.
46. 标准名称, "Information Security Technology – Guideline for Identification of Critical Data", January 7, 2021, available at: www.tc260.org.cn (PDF); 关键信息安全标准使用指南 National Information Security Standardization Committee, September 2021, available at: www.tc260.org.cn (PDF).
47. R. Creemers, "China's Emerging Data Protection Framework", SSRN, November 16, 2021, available at: papers.ssrn.com.
48. 中华人民共和国公安部令, State Council, People's Republic of China, September 15, 2018, available at: www.gov.cn.
49. P. Triolo *et al.*, "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus", DigiChina, Stanford University, August 2021, available at: digichina.stanford.edu.
50. DSL, Article 31.

and industry associations, which issues and publicizes reprimands for violations of personal information protection laws.[51]

Ministry of State Security (MSS)

The MSS, China's foreign intelligence and counter-intelligence service, is another significant actor shaping the security environment in Chinese cyberspace. Alongside the MPS, the MSS has vetting authority over personnel staffing the in-house cybersecurity teams that all CII operators in China are now required to establish.[52] It is associated with the China Information Technology Security Evaluation Centre (CNITSEC), which manages the China National Vulnerability Database for Information Security and conducts software vulnerability testing.[53] In 2003, Microsoft gave CNITSEC limited access to the Windows source code for such testing, which researchers have speculated may have aided the MSS in developing computer network exploitation (CNE) capabilities.[54] In 2021, the US and allied governments accused the MSS of engaging in international CNE for commercial advantage.[55]

Ministry of Foreign Affairs (MFA)

The MFA seems to have asserted itself as the interface for foreign interlocutors in China's cyberspace diplomacy, having previously had to contend with direct interventions by the CAC in international dialogues. The MFA has a dedicated lead for cyberspace diplomacy that was established as a counterpart to the US State Department's Coordinator for Cyber Issues. The MFA leads China's participation in the UN-based dialogue processes for development of international cyberspace norms, and it has developed relevant bodies of in-house expertise.[56]

51. K. Tai, "Chinese Interagency Group Calls Out Apps for Illegally Collecting User Data", DigiChina, Stanford University, July 29, 2019, available at: digichina.stanford.edu; R. Creemers, "China's Emerging Data Protection Framework", *op. cit.*
52. P. Triolo *et al.*, "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus", *op. cit.*
53. J. Chen *et al.*, *China's Internet of Things*, U.S.-China Economic and Security Review Commission, p. 68, available at: www.uscc.gov.
54. J. Lindsay, T. M. Cheung and D. Reveron (eds.), *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford: Oxford University Press, 2015, p. 11.
55. "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China", *Statements and Releases*, The White House, July 19, 2021, available at: www.whitehouse.gov.
56. R. Creemers, "China's Cyber Governance Institutions", *op.cit.*, p. 18.

People's Liberation Army (PLA)

Mention should also be made of the PLA, China's military. 'Military data' is excluded from the DSL's scope, meaning the PLA is not subject to the data management obligations imposed on most other actors. However, the PLA is represented in the CCCI by the Chairman of its General Staff and Vice-Chairman of the Central Military Commission, Xu Qiliang (Xi Jinping's deputy in military command). Military uses of cyberspace are likely to be managed primarily through the PLA's Strategic Support Force and the National Security Commission chaired by Xi Jinping.

China's Regulatory Regime for Cyberspace: Building a Comprehensive System to Monitor and Shape Activity

China's cyberspace governance regime now rests on the legislative pillars of the CSL, DSL and PIPL. These three laws provide the framework for new measures that increasingly focus on managing data and regulating specific activities and economic sectors. Like the institutional architecture described above, this regulatory regime is riddled with underspecified terms and overlapping responsibilities. Nonetheless, it now provides the world's most comprehensive system for a government to monitor, control and shape activity in cyberspace, including by foreign actors within its jurisdiction. It is designed to protect both the interests of private citizens and the public interest as defined by the Party-state, while maximizing the potential of cyberspace to promote economic development.

China's recent and much discussed crackdown on its internet technology firms sits clearly within this framework, being limited in scope and measures to curb these companies' most socially harmful activities. Almost all the associated punitive measures have been directed at the largest internet platform providers, and specifically at activities seen to generate negative social externalities. Such measures can serve both political and technocratic objectives. For example, the discipline exerted against Alibaba and its affiliate Ant Financial, and against Alibaba's former executive chairman Jack Ma, followed Ma's public criticism of government regulators and were likely a warning against challenging the Party-state's authority. However, the regulatory measures targeting Ant Financial's activities were probably also merited to curb injection of risk into China's financial and debt markets. Much of the regulatory action targets monopolistic behavior in the internet technology sector.[57]

57. Q. Chen, "Revised Law: No Leveraging Data or Tech Advantages for Monopoly Position", DigiChina, Stanford University, July 14, 2022, available at: digichina.stanford.edu.

Cybersecurity Law (CSL): Foundational Rules for Securing Cyberspace

The **CSL**, which came into effect in 2017, requires all network operators to participate in the multi-level protection system (MLPS) and undertake measures that include instituting internal security management systems, technical security measures and cybersecurity training. Network operators must 'provide technical support and assistance to public security organs and national security organs', a clause (Article 28) that has drawn much foreign attention in the context of concerns about Chinese espionage and the potential role of Chinese ICT providers like Huawei.[58] The CSL also imposes specific duties on ICT providers, such as complying with mandatory security certification or inspection by state authorities regarding certain categories of equipment and products, requiring users of their services to provide real identity information, and formulating emergency response plans for cybersecurity incidents.[59]

CII operators 'purchasing network products and services that might impact national security' are required to undergo a cybersecurity review organized by the CAC and relevant agencies.[60] This CSL clause (Article 35) was cited as one basis for the review announced by the CAC into the ride-hailing platform provider Didi Chuxing following its 2021 New York Stock Exchange listing. Didi's listing was viewed as problematic by Chinese authorities given the company's possession of large quantities of personal information on Chinese citizens and US government disclosure requirements for listing on US stock exchanges.[61] The cybersecurity review concept introduced by CSL Article 35 has now been expanded to a wide range of situations by subsequent regulations, as described below.

Article 37 of the CSL directs that 'personal information' and 'important data' gathered or produced by CII operators within the territory of mainland China must be stored within mainland China, with export of such data being subject to a security assessment by the CAC and relevant agencies. This obligation regarding data localization and export control has been a major compliance risk issue for foreign actors, given that the CSL does not define 'personal information', 'important data' or 'CII operators', terms that have only recently received more clarity in newer regulations and standards.

58. S. Stolton, "Chinese Cybersecurity Law Is a 'Loaded Weapon,' Senior US Official Says", *Euractiv*, February 27, 2019, available at: www.euractiv.com.
59. CSL Articles 23, 24, 25.
60. "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)", New America, June 29, 2018, available at: www.newamerica.org, Article 35.
61. "Translation: CAC Announces 'Cybersecurity Review' of Ride-Hailing Giant Didi, Just After Its IPO", DigiChina, Stanford University, July 2, 2021, available at: digichina.stanford.edu.

The definition and duties of 'CII operators', for example, were elaborated further by the 'Critical Information Infrastructure Security Protection Regulations' (CIISPR) that came into effect in September 2021, in close sequence with the DSL and PIPL. The CIISPR gives 'guidance and supervisory' responsibility for CII protection to the MPS, but under overall coordination by the CAC, an arrangement that does not clearly resolve bureaucratic turf wars. Relatedly, the CIISPR does not define the relationship between the evolving CII protection regime and the MPS-managed MLPS.[62]

However, the CIISPR does introduce a system of measures for identifying and securing critical information infrastructure, which goes far beyond CII protection steps instituted to date by the EU and US.[63] State agencies are required to develop rules for identifying CII by industry and sector, with operators obliged to notify authorities of changes that bear upon their identification as 'CII operators'. This comes with a range of obligations, which include reporting cybersecurity incidents or threat identification to the CAC and the MPS, supervising their suppliers' compliance with security duties imposed by state regulation, conducting annual CII risk assessments, and establishing dedicated security management bodies staffed with personnel vetted by the MPS and MSS.[64]

In January 2022, the CAC issued a final version of Cybersecurity Review Measures (CRM) that came into effect the following month. The CRM expands the scope of CSL Article 35 to also apply to data handling activities by internet platform providers (IPPs), for example the providers of China's 'super-apps' like Alibaba and Tencent. For both CII operators and IPPs, mandatory self-submission to cybersecurity review by state authorities applies whenever their activities 'affect, or may affect, national security', with risk factors listed (for example, the risk of interference with installed equipment, or reliability of supply accounting for political factors).[65] CII operators must bind their ICT suppliers to cooperate with such state reviews.[66] IPPs that hold personal information of more than one million users and plan to list on foreign stock exchanges must undergo review.[67]

62. P. Triolo *et al.*, "After 5 Years, China's Cybersecurity Rules for Critical Infrastructure Come Into Focus", *op. cit.*
63. *Ibid.*
64. DigiChina, August 18, 2021, *op. cit.*
65. Cyberspace Administration of China (CAC), Cybersecurity Review Measures, January 2022, 网络安全审查办法-中共中央网络安全和信息化委员会办公室, available at: www.cac.gov.cn, Article 2; Article 10(A) and 10(C).
66. *Ibid.*, Article 6.
67. *Ibid.*, Article 7.

Data Security Law (DSL): A Comprehensive Framework for Data Regulation

The DSL, which came into effect in September 2021, is a globally unique project to create a comprehensive regulatory framework for data – excepting only state secrets and military data – that prioritizes national security and social development.[68] The DSL applies to data handling activities within China's mainland territory, defined as 'collection, storage, use, processing, transmission, provision, disclosure, etc.' of 'any information in electronic or other form'.[69] In line with the policy framework described above, the DSL's content is directed at securing data, but also at promoting the use of data as a factor of production by creating institutional frameworks for marketizing it.

The DSL directs the state to devise a categorized and graded system for protecting data according to its 'degree of importance in economic and social development'.[70] It requires the establishment of separate mechanisms for risk assessment, monitoring, information sharing and early warning; for emergency response; and for review on national security grounds, corresponding at least partly with the January 2022 CRM described above. State agencies are to develop catalogues of 'important data' within their areas of responsibility (though guidance for identifying such data remains a work in progress). Decentralizing the definition of 'important data' has the additional benefit of potentially alleviating bureaucratic turf wars over this issue.[71] In July 2022, the lead drafter of TC260's draft 'important data' standard said that a separate standard on 'Security Requirements for Handling of Important Data' was under development, and that in identifying important data, emphasis should be given to the consequence of data mishandling rather than to the type of data being processed.[72]

The DSL also introduces a category of 'core national data', defined broadly in terms of 'national security' and 'public interest', which are to be subject to a stricter management system. The law further devotes a section to government data, which emphasizes not just security measures, but also rights protection and data openness for use 'in service of economic and social development.'[73]

68. R. Creemers, "China's Emerging Data Protection Framework", *op. cit.*
69. DSL, Articles 2 and 3.
70. DSL, Article 21.
71. R. Creemers, "China's Emerging Data Protection Framework", *op. cit.*
72. 如何区分"重要数据"？国标起草人：侧重从"后果角度"识别, 21经济网, available at: www.21jingji.com.
73. DSL, Article 37.

Furthermore, the DSL directs state agencies to establish 'data transaction management systems, standardize data transaction behavior, and cultivate a data transaction market'.[74] These mechanisms complement the PIPL's protections in seeking to regulate China's massive black market in personal information and the social harms it inflicts.[75] They are also directed at persistent organizational and cultural practices that impede data sharing in China, reportedly even within leading platform firms.[76] By one estimate, China will produce a quarter of the world's data by 2025.[77] The DSL entrenches a nation-wide bureaucratic focus on exploiting this resource by requiring the state to support measures for data-related standardization, research, education, innovation, infrastructure building and public service provision. These provisions support state interventions for market optimization, which now include an open national data-sharing platform and have foreign counterparts in forthcoming EU legislation.[78]

The DSL directs implementation of a system of data export controls, though the relationship to the cybersecurity review process described above or to China's 2021 unified export control law remains unclear. It circumscribes provision of data to foreign authorities in equivalent terms to the PIPL.[79] But the DSL's extraterritorial jurisdiction is more sweeping than the PIPL's, covering data handling activities outside China's territory that 'harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC.' 'National security' is left undefined, but the term has been given broad meaning in other Chinese laws and authoritative policy statements.[80] The DSL's liability regime deals specifically with cross-border provision of 'important data' collected or produced by CII operators that is non-compliant with the CSL-based data export regime.

Some DSL provisions received more articulation in November 2021 with release of draft Online Data Security Management Regulations (ODSMR).[81] These draft lists prohibited activities and obligations for data

74. DSL, Article 19.
75. See e.g. E. Tham, "Data Dump: China Sees Surge in Personal Information Up for Sale", Reuters, August 23, 2018, available at: www.reuters.com.
76. See e.g. C. Cheng and I. Deng, "Tencent Seeks to Kill Silo Culture That Gave It WeChat as It Expands into AI, Big Data", *South China Morning Post*, November 14, 2018, available at: www.scmp.com.
77. S. Radu, "Which Country Owns Data? Increasingly, It's China", *US News*, February 14, 2019, available at: www.usnews.com.
78. Q. Chen, "China Wants to Put Data to Work as an Economic Resource—But How?", DigiChina, Stanford University, February 9, 2022, available at: digichina.stanford.edu.
79. DSL, Article 36.
80. See e.g. the 2015 National Security Law available at: www.chinalawtranslate.com; Xi Jinping, 2014, "Maintain an Outlook of Comprehensive National Security, Walk the Path of National Security with Chinese Characteristics" 习近平：坚持总体国家安全观 走中国特色国家安全道路-高层动态-新华网, available at: www.xinhuanet.com.
81. "Translation: Online Data Security Management Regulations (Draft for Comment) – Nov. 2021", DigiChina, Stanford University, December 6, 2021, available at: digichina.stanford.edu.

handlers, and requires handlers of 'important data' to establish an in-house data security management body with specified duties, such as filing reports with local authorities containing specified content, including the storage methods and location of the important data.[82]

The ODSMR further expands the scope of CSL Article 35, requiring cybersecurity reviews in the following situations:

a) where Internet platform operators collecting or holding large amounts of data resources related to national security, economic development, or the public interest, carry out mergers, reorganizations, or separations, affecting or possibly affecting national security;

b) where data handlers handling personal information of more than 1 million individuals list on a market abroad;

c) where data handlers list in Hong Kong, affecting or possibly affecting national security;

d) other data handling activities affecting or possibly affecting national security.[83]

Furthermore, the draft ODSMR asserts wide extraterritorial jurisdiction, applying to activities outside China that involve handling the data of Chinese citizens or organizations where such handling:

a) involves 'important data' within China;

b) is for the purpose of providing products or services within China;

c) analyses behavior of individuals or organizations within China;

d) as provided for by other Chinese laws or administrative regulations.[84]

82. DigiChina, December 6, 2021, *op. cit.*, Article 29.
83. DigiChina, December 6, 2021, *op. cit.*, Article 13.
84. DigiChina, December 6, 2021, *op. cit.*, Article 2.

Personal Information Protection Law (PIPL): Controlling Abuse of Personal Information

The PIPL is the outcome of China's slow evolution from sectorally-fragmented regulation of data protection towards a universal regime that regulates personal information as a distinct category.[85] It addresses popular demand in China for more effective protection of personal data, in the face of widespread abuses by non-state actors. It also reflects international recognition of this issue's importance that is increasingly expressed in regulation elsewhere, most notably the EU's GDPR.

The PIPL applies to handling of personal information of 'natural persons' within China's borders. It distinguishes between 'data handlers' and 'entrusted persons', roughly analogous to 'data controllers' and 'data processors' under the GDPR.[86] Like the GDPR, the PIPL asserts extraterritorial jurisdiction over activities outside China 'where the purpose is to provide products or services' or 'is analyzing assessing activities' of natural persons inside China.[87] The data localization requirement for personal information in CSL Article 37 is linked to quantitative thresholds to be specified by the CAC, while state organs handling personal information must store it inside China.[88] The PIPL's provisions concerning cross-border data export are discussed below.

Rather than creating fundamental rights or general legal principles, the PIPL regulates categories of actors and their relations based on judgments about applicable risks and harms.[89] It recognizes a range of legitimate reasons for handling personal information in addition to individuals' consent, for example on contractual bases and 'to fulfill statutory duties and responsibilities'.[90] There is a general requirement for personal information handlers to give individuals prior notification of certain details, notably the purpose and methods of the handling.[91] Large platform operators are given extra duties, while state agencies are directed to formulate specialized (and presumably less burdensome) rules and standards for small-scale personal information handlers.[92] The PIPL has specific provisions for personal

85. R. Creemers, "China's Emerging Data Protection Framework", *op. cit.*; E. Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?", *Penn State Journal of Law & International Affairs*, Vol. 8, No. 1, pp. 49-117.
86. A. Lee, "Personal Data, Global Effects: China's Draft Privacy Law in the International Context", DigiChina, Stanford University, January 4, 2021, available at: digichina.stanford.edu.
87. PIPL, Article 3.
88. PIPL, Articles 40 and 36.
89. R. Creemers, "China's Emerging Data Protection Framework", *op. cit.*
90. PIPL, Article 13.
91. PIPL, Article 17.
92. PIPL Articles 58 and 61.

information handling by state organs, which are generally subjected to the universal duties.

The extent to which the PIPL's protections prove enforceable in practice against state agents will determine whether China moves away from a 'dichotomy between privacy from private actors and privacy from the state'.[93] State organs' handling of personal information is made subject to legal regulation and the scope of their responsibilities, and individuals are given the right to file legal suit for rights violations by personal information handlers. Unlike the GDPR, the PIPL does not establish any independent data protection authority: the CAC has both policymaking and oversight authority concerning its provisions.[94]

Some of the PIPL's protections and enforcement measures go significantly beyond the GDPR. The PIPL's consent requirements are notably more burdensome than the GDPR's.[95] In defining 'sensitive personal information' subject to additional safeguards, the PIPL takes a risk-based approach that is broader than the GDPR equivalent.[96] The PIPL's non-compliance penalties include personal sanctions for company officers and fines of up to 5% of annual revenue.[97]

Toward an Intrusive Regime to Control Cross-border Data Transfers

In July 2022, the CAC published finalized Outbound Data Transfer Security Assessment Measures (ODTSAM) that take effect from 1 September 2022, with a six-month grace period provided for extant cross-border data transfer activities to be made compliant with the ODSTAM's provisions.[98] The ODTSAM integrates and articulates obligations across the CSL, DSL and PIPL concerning data export outside of China.[99] It requires all data handlers to conduct their own compliance assessment for any cross-border data transfer.[100] The additional obligation of a state-conducted cybersecurity review grounded in CSL Article 35 will apply to cross-border transfers in four circumstances:

93. E. Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?", *op. cit.*, p. 116.
94. A. Lee, "Personal Data, Global Effects: China's Draft Privacy Law in the International Context", *op. cit.*
95. *Ibid.*
96. E. Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?", *op. cit.*, pp. 95-96; PIPL, Article 28.
97. PIPL, Article 66.
98. "Translation: Outbound Data Transfer Security Assessment Measures – Effective Sept. 1, 2022", DigiChina, Stanford University, July 8, 2022, available at: digichina.stanford.edu.
99. S. Sacks *et al.*, "Knowns and Unknowns About China's New Draft Cross-Border Data Rules", DigiChina, Stanford University, November 5, 2021, available at: digichina.stanford.edu.
100. ODTSAM, Article 5.

1) Where the data handler provides important data abroad;

2) Critical information infrastructure operators and data handlers handling the personal information of over 1 million people providing personal information abroad;

3) Data handlers providing abroad the personal information of more than 100,000 people or the sensitive personal information of more than 10,000 people since January 1 of the previous year;

4) Other circumstances where the CAC provides that data export security assessment must be applied for.[101]

The ODTSAM does not resolve the ambiguity described above in extant guidance on defining 'CII operator' and 'important data'. Nor does it define the terms 'providing abroad' or 'data export', actions which attract cybersecurity review.[102] Additionally, the ODTSAM makes no reference to the 'core national data' category introduced by the DSL. However, the ODTSAM does list the main criteria applicable to cybersecurity review, which notably include the cybersecurity environment (including policies and regulation) of the country or region where the receiving party resides, and whether data security responsibilities are stipulated by the contract between the data handler and the receiving party. The required content for such contracts is also articulated, as are timeframes and validity periods for the state's cybersecurity reviews, and circumstances triggering re-evaluation.

Regarding personal information, the PIPL provides additional grounds for legitimate cross-border transfer: 1) 'undergoing personal information protection certification' under rules yet to be issued, (2) using a standard contract to be formulated by the CAC for cross-border transfers, (3) as provided for by international agreements concluded by China. The last criterion probably signals an intention to negotiate blanket cross-border transfer agreements with foreign jurisdictions, which aligns with China seeking to join existing multilateral trade treaties that deal with cross-border data flows.[103] Personal information stored within China cannot be exported to foreign judicial or law enforcement authorities without approval from Chinese authorities, even where an international treaty applies.[104] Regarding the second criterion, in June 2022 the CAC released for public comment a draft standard contract for cross-border transfers of personal information.[105]

101. ODTSAM, Article 4.
102. S. Sacks *et al.*, "Knowns and Unknowns About China's New Draft Cross-Border Data Rules", *op. cit.*
103. *Ibid.*
104. PIPL, A41.
105. 国家互联网信息办公室关于《个人信息出境标准合同规定（征求意见稿）》公开征求意见的通知, Ministry of Justice, People's Republic of China, June 30, 2022, available at: www.moj.gov.cn.

These rules place a heavy compliance burden on entities seeking to regularly transfer data out of China. In the context of long-running debates within Chinese officialdom over the desirable balance between informatization and security, the emerging cross-border transfer regime seems weighted towards the latter.[106] Rather than winding back these general requirements, future compromises to facilitate cross-border economic activity will more likely be expressed through special provisions for China's most technologically advanced and internationally connected cities. Several subnational jurisdictions are trialing localized cross-border data transfer regimes, within the framework of a continuing pilot program to develop trade in innovative services in selected locations around China.[107] Beyond these regionally confined regimes, the national regime seems increasingly to be directed at effectively coercing data localization within China's borders, including by foreign entities, for large volumes of personal information or for 'important data' as defined by state authorities.

106. S. Sacks, P. Triolo and G. Webster, "Beyond the Worst-Case Assumptions on China's Cybersecurity Law", New America, October 13, 2017, available at: www.newamerica.org.
107. "GIZ Industrie 4.0 Project – Policy Briefing on Cross-Border Data Transfer Piloting – Focus on Hainan Free Trade Port", *Plattform Industrie 4.0*, Federal Ministry for Economic Affairs and Climate Action, December 15, 2020, available at: www.plattform-i40.de.

Conclusion: Future Trends and Lessons for Europe

The ambition and iterative development of China's emergent governance regime for cyberspace have inevitably had some retarding effects on its commercial development. Reported complaints are numerous in China about the various measures' lack of rationality, and the government's apparent lack of forethought about their negative second-order effects.[108] For instance, in March 2022 a senior researcher at a Ministry of Commerce-affiliated institute claimed that lack of policy coordination, regulatory duplication and excessive controls over data were hurting development of China's digital economy and the international competitiveness of its internet technology firms.[109]

The vast potential scope of the national security-related basis for state intervention, including through the exercise of extraterritorial jurisdiction, is likely to have a chilling effect, especially on international exchanges. The compliance burden for cross-border transfers of 'sensitive personal information' or 'important data' is already onerous enough to incentivize data localization: for example, there is no time limit for reviews of applications for cross-border data transfer, which can be extended at CAC's discretion.[110] Foreign entities doing business with or in China will need to bear this regulatory risk simply to continue operations, given the nation's pace of regulatory innovation.

China now has sectoral data protection regimes for banking, healthcare, automobiles and recommendation algorithms. Broader implementations of the regulatory framework are under development, such as MIIT's trial Data Security Management Measures for Industry and Information Technology.[111] Rapid evolution in China's system of technical standards is further shaping the way these rules are implemented.[112] In July 2022, fifteen Chinese agencies including the CAC published a plan to develop standards across China's economy, including standards governing data transactions.

---

108. See e.g. C. Che and J. Goldkorn, "China's 'Big Tech Crackdown': A Guide", *op. cit.*
109. Chinese Academy of Fiscal Sciences, March 4, 2022, available at: www.chineseafs.org.
110. ODTSAM, Article 12.
111. R. Creemers, "China's Emerging Data Protection Framework", *op. cit.*;
公开征求对《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》的意见, Ministry of Industry and Information Technology, October 29, 2021, available at: wap.miit.gov.cn.
112. J. Lee, E. Zhang and R. Creemers, "China's Standardisation System – Trends, Implications and Case Studies in Emerging Technologies", *op. cit.*

The reality is that China's economic and security needs in cyberspace required a sweeping regulatory response, which has been messy in execution but will likely stabilize the environment and ensure it conforms to the Party-state's policy priorities, including its imperative for political control. This governance regime has emerged progressively, in response to a course of cyberspace development that has immensely benefited China, but has also generated significant social harms, diverted resources from development of 'core technologies', and exposed the nation to a range of economic and security risks. The key issue now is to what extent such a comprehensive, intrusive and onerous regime can be reconciled to cross-border connections, in a context where there are already many pressures pushing foreign actors to 'decouple' from China.

China's cyberspace governance system is unlikely to be rolled back in response to changing circumstances, whether this means falling market values for internet platform companies, US restraint from further measures targeting China's technological progress, or the end of Xi Jinping's leadership. Rather, it should be expected to continue expanding, giving the Party-state more visibility and tools of control over activity on China's digital networks, and increasingly over foreign activity that impacts upon Chinese cyberspace. Yet China's leaders are also determined to maintain the Chinese economy's international links, as evident in the agenda they brought to the top-level summit with EU leaders in April 2022.

Maintaining large volume data flows between China and the EU may require a bespoke agreement, comparable to the new data privacy framework recently agreed with the US.[113] Given EU judicial authorities' interpretation of the GDPR, requiring 'essentially equivalent' protections to be provided by foreign governance regimes, it may be up to individual EU member-states to force sectoral carve-outs from EU law, such as for national security matters regarding data exchanges with the US.[114] The prospects of this happening for China, or for its data regime being viewed by European data protection authorities as providing equivalent protections to those of the EU, are not good.

Those doing business with China must also account for the Party-state's increasing readiness to use punitive economic measures in response to actions by other governments. This trend will be reinforced by threat perceptions of potential state-imposed sanctions on the scale currently

113. "FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework", Statements and Releases, The White House, March 25, 2022, available at: www.whitehouse.gov.

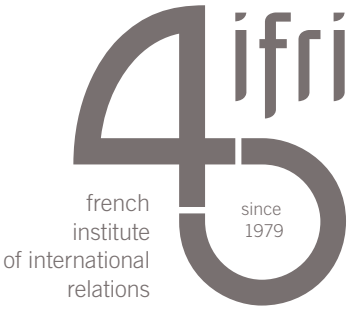
114. J. Lee, "Blocking the Flow: Data legislation and the EU-US-China triangle", *Transatlantic Dialogue on China Blog*, RUSI, April 15, 2021, available at: www.transatlantic-dialogue-on-china.rusi.org; T. Christakis and K. Propp, "How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States", *Lawfare*, March 8, 2021, available at: www.lawfareblog.com.

being applied to Russia. While foreign ICT companies are unlikely to abandon China as readily as Russia, Chinese authorities can be expected to prioritize pre-emptive deterrence of foreign firms choosing market exit during a crisis. In 2021 China adopted a Law for Countering Foreign Sanctions, and its new cyberspace regulatory regime provides for punishing foreign actors in defense of Chinese interests, even if they are not individually associated with the offending behavior.

For example, PIPL Article 42 empowers the CAC to put foreign entities on a blacklist that limits or prohibits access to personal information from China. Both the PIPL and DSL provide for reciprocal retaliation by Chinese authorities against discriminatory measures taken by foreign jurisdictions against Chinese interests.[115] Such provisions unavoidably raise the risks for foreign businesses engaged in intensive information transfers with China, of which there are still many significant European examples. The German electronics giant Siemens for instance operates 20 research and development centers in China, including its global headquarters for robotics research.[116]

Yet despite the shadow it is casting over China's continued integration with the outside world through digital networks, China's cyberspace governance regime also offers constructive lessons. Western countries are engaged in their own political and regulatory responses to the harms caused by unregulated growth of internet platform firms, to the various public and private security threats enabled by the internet, and to the opportunities offered by development of new ICT-enabled technologies. They should observe how China's progress in these fields is affected by its intensive approach to cyberspace management, which is top-down but also decentralized and adaptable to conditions. Achieving the right balance in cyberspace governance will be critical to other countries seeking to protect their interests in an increasingly competitive and digitally connected world.[117]

115. PIPL, Article 43; DSL, Article 26.
116. B. Pongratz, B. Bartch and V. Brussee, "Germany: Politics Trying to Break Free from the Narrative of Economic Dependence", in: J. Seaman *et al.* (eds.), *Dependence in Europe's Relations with China*, European Think-tank Network on China, April 2022, available at: www.ifri.org.
117. J. Lee, E. Zhang and R. Creemers, "China's Standardisation System – Trends, Implications and Case Studies in Emerging Technologies", *op. cit.*



27 rue de la Procession 75740 Paris Cedex 15 – France

Ifri.org