

China's Approach to Cyber Sovereignty

Rogier Creemers



China's Approach to Cyber Sovereignty

Rogier Creemers

Imprint

Published by:

Konrad-Adenauer-Stiftung e. V. 2020, Berlin

Contacts at the Konrad-Adenauer-Stiftung:

Sebastian Weise

Policy Advisor for Innovation

sebastian.weise@kas.de

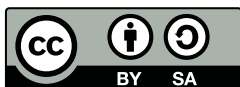
Jason Chumtong

Policy Advisor for Artificial Intelligence

jason.chumtong@kas.de

Cover Image: © Bill Hinton Photography/gettyimages
Design and typesetting: yellow too Pasiak Horntrich GbR

This publication was published with financial support
of the Federal Republic of Germany.



This publication is published under a Creative Commons License:
CC BY-SA 4.0 international (<https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

ISBN 978-3-95721-798-1

At a Glance

Over the past 25 years, China has systematically promoted the introduction and deployment of digital technologies in all areas of the social, economic and political life.

A cornerstone of China's digital policy is the concept of cyber sovereignty, which shapes its domestic policy as well as its digital and cyber diplomacy on the international level. With this approach, China shapes the digital transformation while preserving and strengthening existing political structures.

In global circles, China is pushing for a state-centered, Westphalian understanding of sovereignty, in which the state holds ultimate authority in the digital space. Consequently, every state shall have the right to establish national online spaces and fully control content and data flows within its borders.

China has sought to realize this vision by growing its own regulatory and technological capabilities. It imposes greater controls on international data flows, online content and technology vendors, amongst others. It also focuses on further strengthening its autonomy and self-sufficiency in the digital realm in order to reduce dependencies on innovations from foreign digital providers, thus following the indigenisation approach.

Europe must find adequate answers to China's rise as a digital power. To successfully achieve this goal and maximize the already very limited ways Europe has to influence the People's Republic, understanding its digital policy is essential.

Table of Contents

List of Abbreviations	5
1. Introduction	6
2. The Origins and Key Elements of China's Conception of Cyber Sovereignty	8
3. Sovereignty in the International Sphere	11
4. Defending Sovereignty at Home: Territorialisation and Indigenisation	13
5. Conclusion	19
References	22
Author	26

List of Abbreviations

CAC	Cyberspace Administration of China
CETC	China Electronics Technology Group
CNITSEC	China Information Technology Security Evaluation Centres
CNNIC	China Internet Network Information Centre
CSL	Cybersecurity Law
DNS	Domain Name System
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IoT	Internet of Things
ITU	International Telecommunication Union
MLPS	Multi-Level Protection System
OEWG	Open-Ended Working Group
TOR	The Onion Router
UN	United Nations
UN GGE	United Nation's Group of Governmental Experts
VPN	Virtual Private Network
WAPI	WLAN Authentication and Privacy Infrastructure
WSIS	World Summit On the Information Society
WTO	World Trade Organization
ZUC	Zaurus Unit Converter

1

Introduction

Over the past 25 years, China has enthusiastically supported the adoption and expansion of digital technologies in all areas of social, economic and political life. While the country was a relative latecomer to connectivity, only gaining full access to the Internet in 1994, it now boasts over 900 million users, the world's largest online population. It is the only country with a digital economy comparable to that of the United States. Of the 30 largest Internet businesses by market value, nine are Chinese. Huawei has become the world's largest smartphone manufacturer, as well as a leader in 5G mobile infrastructure. China is a forerunner in numerous technologies, including online payment and e-commerce, and has ambitions to become a global leader in core technologies of the future, including artificial intelligence and quantum computing.

China has, however, achieved these successes without adopting the values of the free and open Internet as espoused in the West, which were considered crucial for the development of a successful digitised sector. Instead, from the late 1990s onward, successive measures were taken to control online content, the best-known of which is the Great Firewall, which filters and blocks undesired foreign websites. More recently, Beijing has taken active measures to advance local businesses and support home-grown technology, and currently pursues a policy of greater technological self-reliance.

These measures are all elements of the policy principle of “cyber sovereignty” (*wan-gluo zhuquan* 网络主权). Although sovereignty concerning digital affairs only became part of policy jargon in 2010, it reflects a deep undercurrent in Chinese foreign policy that has existed since the earliest days of the People's Republic. In this view, it is the leadership's task to ensure that China can achieve its development objectives without being subject to interference from foreign governments, particularly those “foreign hostile powers” who are deemed to conduct “strategies and plots to Westernise and divide our country” (Hu 2011).

By now, cyber sovereignty has become the cornerstone of China's stance in global cyber diplomacy, as well as the animating principle for its domestic digital policies. It shapes China's participation in international processes under the United Nations umbrella and organisations such as ICANN, as well as the formulation of regulations for content control, data protection, product certification and critical infrastructure protection. At the domestic level, it has become the cornerstone of increasingly stringent laws, regulations and policies that aim to enhance the Chinese government's ability to control online processes, increasingly indigenise software and hardware value chains, and enhance strategic autonomy. Given China's position as the emerging leader in the digital world, its interpretation of cyber sovereignty will inevitably impact the global cyber order. An accurate understanding of China's objectives and concerns, its view of the cyber world and the challenges it faces, is essential for policymakers, businesses and observers in order to anticipate and respond to Beijing's increasingly assertive stance. To this end, this report will survey three elements of China's cyber sovereignty approach. First, it will discuss how the notion of sovereignty in cyberspace emerged historically, and how it shapes China's broad

strategic agenda. Second, it will review how China has sought to reorient international cyber governance and diplomacy processes to better reflect this agenda. Lastly, it will assess how China has progressively attempted to realise the key tenets of cyber sovereignty domestically, focusing specifically on content control, data protection and the preferential treatment of domestic businesses.

Some sections of this report draw on a previously published book chapter: Creemers, Rogier. 2020. "China's Conception of Cyber Sovereignty: Rhetoric and Realisation." In: Broeders, Dennis and Bibi van den Berg (eds.) *Governing Cyberspace: Behavior, Power and Diplomacy*. Rowman & Littlefield.

2

The Origins and Key Elements of China's Conception of Cyber Sovereignty

While cyber sovereignty itself only became a widely used policy term in a 2010 governmental whitepaper, it draws on a long-held prioritisation of sovereignty in Chinese policy that emerged soon after the People's Republic was founded in 1949. The Five Principles of Peaceful Coexistence, which are still the cornerstone of Chinese foreign policy, list 'respect for national sovereignty' first (Kent 2008). The roots for this stance lie in China's often painful encounter with imperial powers, and its struggle to achieve modernisation. Throughout the second half of the 19th century, foreign military intrusion and growing domestic crises combined to erode the integrity of the Qing Empire. Successive generations of intellectuals and officials sought ways to first reform the imperial architecture, and after it fell, create a new governing structure to restore China to a position of "wealth and strength" (*fuqiang*, Schell and DeLury 2014). While this search included the importation and translation of Western political works, the experience of imperialist intrusion and China's failure to regain German-held concessions at the Versailles conference drove political leaders away from the West and towards the newly established Soviet Union. Republican leader Sun Yat-sen reorganised his political party along explicitly Leninist lines, and the Chinese Communist Party was established with Soviet assistance in 1921, espousing an explicitly sovereignty-oriented and anti-imperialist foreign policy doctrine.

Where the initial project of sovereignty was to eliminate foreign imperialist authority and influence in China, the dynamics of 1989 created a new strategic environment, and concomitant challenges for Beijing. Both the wave of domestic protests and the rapid disintegration of the Soviet Union and its satellites rattled the CCP leadership, and maintaining political stability became the overarching concern animating party policy. Specifically, the leadership diagnosed that Western attempts at Peaceful Evolution and Ideological Diversion had been an important factor driving both the escalation of unrest at home, and eroding support for the socialist system in the Eastern Bloc. In the subsequent decades, it particularly came to see the United States as an existential threat: American support for regime change and colour revolutions across the globe would be seen in Beijing as a precursor to subversion in China. As the Party's chief theoretical journal *Qiushi* put it: "As a Socialist country under the leadership of the Communist Party, China will face the pressure of Western containment and forcible change for a long time, and ideological infiltration is the main method of Western hostile forces to implement a strategy of westernisation and division in our country" (Qiushi 2013). To be sure, the objective of this narrative is to be politically useful, rather than historically accurate, and China has not always faithfully observed its own norm of non-interference. Nevertheless, it contains important pointers towards the CCP's self-image that help interpreting the specifics of sovereignty in cyberspace.

China's view of sovereignty explicitly rejects key, substantive elements of the post-Cold War worldview that had been dominated by liberal ideas, most notably the universality of human rights and democratisation (Zhang 2013), as well as the importance of international organisations empowered to interfere into countries' domestic affairs. As digital technology emerged and grew in popularity and adoption, these pre-existing

policies were expanded to include the online world, focusing first on content. Invoking Cold War-era ideas concerning "Peaceful Evolution", China views foreign media as part of an attempt at ideological intrusion, aimed at subverting the Party's authority. Over the years, concerns have broadened to encompass data, supply chain and critical infrastructure security, and the global internet governance architecture. Increasing technology-related tensions with the United States, as evidenced recently by US export sanctions against several Chinese businesses, have exacerbated Beijing's sense of urgency to attain strategic autonomy. But how is cyber sovereignty currently defined? The most comprehensive description can be found in the 2017 International Strategy on Cooperation in Cyberspace:

» *"As a basic norm in contemporary international relations, the principle of sovereignty enshrined in the UN Charter covers all aspects of state-to-state relations, which also includes cyberspace. Countries should respect each other's right to choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs, or engage in, condone or support cyber activities that undermine other countries' national security.*

Upholding sovereignty in cyberspace not only reflects governments' responsibility and right to administer cyberspace in accordance with law, but also enables countries to build platforms for sound interactions among governments, businesses and social groups. This will foster a healthy environment for the advancement of information technology and international exchange and cooperation.

National governments are entitled to administer cyberspace in accordance with law. They exercise jurisdiction over ICT infrastructure, resources and activities within their territories, and are entitled to protect their ICT systems and resources from threat, disruption, attack and destruction so as to safeguard citizens' legitimate rights and interests in cyberspace. National governments are entitled to enact public policies, laws and regulations with no foreign interference. Countries should exercise their rights based on the principle of sovereign equality and also perform their due duties. No country should use ICT to interfere in other countries' internal affairs or leverage its advantage to undermine the security of other countries' ICT product and service supply chain." (MFA 2017).

While China's definition of cyber sovereignty remains vague, the International Strategy on Cooperation in Cyberspace and accompanying documents nevertheless can be unfolded along four important dimensions.

The first is the *target* of sovereignty, or, who the claim of sovereignty is aimed at. On the one hand, China claims supreme national authority against foreign governments, rejecting the applicability of universal rights as well as foreign attempts to intervene in its own internal affairs. On the other hand, it targets non-governmental actors, including businesses, the technology community and civil society. This opposes the multi-stakeholder model for cyber governance that characterises institutions such as ICANN and the IETF, and which has been espoused by WSIS and the IGF. Instead,

China advocates that international cyber diplomacy and governance processes should be brought into the fold of the United Nations.

The second dimension is the *nature* of the sovereignty claim. On the one hand, it constitutes a claim to a specific legal entitlement: it should be recognised in international law that governments hold supreme authority within their national cyberspace. Yet in the absence of international agreement to that effect, China has also sought to develop the real-life capability to ensure its ability to uphold sovereignty.

The third dimension concerns the *objectives* of the pursuit of sovereignty, which primarily include territorialisation and indigenisation. With territorialisation, Beijing seeks to delineate its national boundaries in cyberspace, ensure that online processes affecting important Chinese interests take place within those boundaries, and unwanted activities can be barred from entering. Indigenisation, in turn, attempts to substitute foreign actors and technologies by homegrown equivalents, reducing reliance on the outside world and building a competitive digital sector.

The fourth dimension consists of the *means* to realise sovereignty, which can be divided into legal-regulatory tools that enhance territorialisation and indigenisation through rules governing digital activities, and policy support and investment instruments that directly support the development of China's digital capabilities through mechanisms ranging from greater education, research and development funding to infrastructure construction, government procurement and the establishment of specific investment channels and vehicles.

3

Sovereignty in the International Sphere

In the international sphere, China's push for sovereignty has, on the one hand, consisted of efforts to promote its stance in several ongoing diplomatic cyber governance processes, most notably in the United Nations, and on the other hand to push for the reform of existing organisations, such as ICANN and the International Telecommunications Union (ITU), to align more closely with Chinese preferences. Throughout, China has been closely aligned with Russia, and these two countries are often considered as the core of a group of countries opposing the "like-minded" grouping of states formed by Western countries. In the beginning, a lack of diplomatic experience meant China was often a junior and more reticent partner in this relationship. More recently, however, China has become more vocal and assertive about its objectives and interests, even as it maintains a close diplomatic association with Moscow (Broeders et al. 2019).

In the United Nations, China has come quite a long way since the first rounds of UN GGE negotiations, where it had sent ill-prepared officials from the Trade Ministry to discuss tough security questions. It established a cyber coordination office within the Arms Control Department of the Ministry of Foreign Affairs, with the express mandate to represent China in cyber diplomatic processes. Together with Russia and other fellow wayfarers, China managed to include in the 2013 UN GGE report stipulations concerning the recognition of the sovereignty principle and that "the international norms and principles that flow from it apply to state[s]' conduct of ICT-related activities." Yet in a subsequent round in 2017, disagreements concerning interpretations of international law on the use of force, self-defence, state responsibility and humanitarian obligations between the Western-orientated like-minded states on the one hand and China, Russia and Cuba on the other, led to a breakdown of the UN GGE mechanism. China voted against a 2018 US-sponsored resolution to instate a next GGE round (which was nonetheless passed), and supported a Russian initiative to establish the Open Ended Working Group (OEWG) on cyber affairs, potentially open to all UN members (Bozhkov 2020). At the first session of this OEWG, China submitted – for the first time – a detailed document outlining a broad agenda with demands going far beyond the classical cybersecurity debate, also including claims concerning supply chain security and the limitation of export bans (MFA 2019). At the same time, the Chinese government insisted that the participation of non-governmental organisations was limited to the greatest possible extent.

China similarly gained greater experience in other organisations. Its initial engagement with ICANN, for instance, was not always harmonious: Beijing boycotted ICANN's Government Advisory Committee for years over disagreement on the status of Taiwan. More broadly, the multi-stakeholder nature of ICANN governance as well as its close relationship with the United States government rankled Beijing, leading it to advocate bringing ICANN into the fold of the United Nations' International Telecommunications Union (Mueller 2012). Recognising the growing importance of China in global cyber affairs, ICANN and its officials went to considerable lengths to build confidence: ICANN opened its first Global Engagement Centre in Beijing in 2013, and then-CEO Fadi Chehadé joined the advisory council of the Wuzhen Initiative at China's flag-

ship cyberspace event. China welcomed ICANN's transition away from US government oversight, even if the new solution stops short of China's preferred option. Nonetheless, China remains worried that the US government might still use residual control over ICANN to target the functioning of Chinese networks.

In terms of efficacy, China's track record in global cyber diplomacy presents a mixed picture. It has been successful in some respects, most notably in the inclusion of sovereignty-related language in the GGE. Moreover, it is often underestimated in the West how attractive the Sino-Russian project of anti-US hegemonism is to third parties, as evidenced by the broad support for telecommunication regulation reforms both countries proposed in the 2012 ITU meeting (Klimburg 2013). The OEWG similarly provides a space where, under the guise of sovereign equality of states, Beijing and Moscow believe they hold greater advantages. Yet at the same time, China's hard line reading of sovereignty has – ironically – pushed other countries to adopt similar positions. Where China has banned foreign content for years, concerns about data transfers to Beijing are now leading to debates about banning Chinese-developed apps such as TikTok in the US and European countries. As China is seeking to reduce reliance on imported technology, Huawei is equally facing increasing headwinds in global markets. As distrust between Beijing and Washington has grown, decoupling has become a major discussion topic in boardrooms and government departments. In other words, Beijing's strict insistence on sovereignty may well turn out to generate significant self-harming consequences. What this will mean for the future of the globally integrated Internet can only be speculated at this point, but some observers are already employing terms such as the Sino-US Tech Cold War, and Innovation Winter (Houser, forthcoming). While the brunt of these tensions lies across the Pacific, this will also have major consequences for Europe. Without a comprehensive digital industry of its own, European governments, at the national and EU level, will have to consider whether to deploy industrial policy to develop one, or have to rely on imported technology. This risks, in turn, the exacerbation of existing fault lines within the Union.

4

Defending Sovereignty at Home: Territorialisation and Indigenisation

To recapitulate: China's perspective on sovereignty in cyberspace is mainly defensive: it serves to protect the integrity of China's political, social and economic architecture against hostile subversion attempts by foreign governments, in particular the United States. At the international level, it seeks to steer away from a governance architecture characterised by strong substantive norms and powerful international institutions, towards a more Westphalian system based on national self-determination and non-interference. Even so, this stance has major international ramifications, as Beijing works to build diplomatic consensus with other nations sharing its view, as they successfully did at the 2012 World Conference on International Telecommunications. Moreover, regardless of circumstances at the international level, Beijing has initiated numerous domestic measures and policies over the past years to enhance its capabilities to realise sovereignty, either through regulatory means or through direct support and investment for education, research, development and industry. These measures either intend territorialisation, ensuring that online activities affecting China take place within its territories, and indigenisation, ensuring that they are performed by Chinese actors using Chinese technologies. This section will review these measures, as well as outline the international debates and trade-offs they involve.

Content

As then-CAC director Lu Wei stated in 2013, China views cyberspace as an extension of the physical world, implying that national borders exist in the virtual environment as well as in the real one (Lu 2013). Yet as the technical functioning of the Internet is geography-agnostic, China has had to erect technological and regulatory boundaries to keep certain processes out, and others in. The best-known of these is the Great Firewall. It was established in early 2000 as part of the Falun Gong crackdown, and has been repeatedly upgraded over the years to ensure that content and online tools that Beijing deems undesired, are not available to Chinese citizens. It blocks explicitly political content, such as references to Falun Gong, the Tibetan or Uyghur cause, and the events of June 1989. Numerous foreign media outlets reporting critically on China, such as the New York Times and the Guardian, have also successively become unavailable. In the wake of the Arab Spring and colour revolutions in ex-Soviet states, social media platforms that had been used in the organisation of these events were blocked (Griffiths 2019). Certain upgrades have also targeted circumvention software: particular commercial VPN services work less effectively around major national celebrations, and TOR, which enables anonymous and encrypted web access, does not function reliably from China.

Complementary to the technical functioning of the Great Firewall, a raft of laws and regulations effectively make it unlawful for foreign online content providers to operate in China. When China joined the WTO in 2001, its services schedule explicitly limited market access for many media-related activities. Subsequent regulations outlawed foreign participation in the production of news content, online publishing and

the provision of online content. As a result of these measures, no foreign operator has been able to acquire and maintain a significant presence on the Chinese market. Only a few foreign entries figure on a top 100 list of mobile apps as measured by market penetration (Jiguang n. d.). Instead, China's online space is dominated by the home-grown giants Baidu, Alibaba and Tencent. In other words, content control measures not only generate direct political benefits, they have also created a favourable environment conducive to the development of domestic counterparts. These have developed a mutually beneficial strategic relationship with government, and assist the realisation of China's developmental aim to move up the economic value chain.

Domain names and traffic

As indicated above, Chinese authorities have often viewed the architecture of the DNS as run by ICANN with suspicion. While pushing for reform at the international level, it has also taken several measures to mitigate the risk this architecture posed in Beijing's view. Almost from the start, the management of domain names became a government affair, in contrast to the multi-stakeholder approach adopted elsewhere. In 1997, the newly established China Internet Network Information Centre (CNNIC), under the Chinese Academy of Sciences, became responsible for managing the Chinese aspects of the DNS, including administration of the .cn domain (Xue 2004). Successive regulations promulgated in 2002 and 2004 started to extend Chinese jurisdiction over the Domain Name System, referring consistently to "our country's Domain Name System". Not only did they encourage the adoption of Chinese-language domain names, they also applied pre-existing provisions on content censorship to domain names, and required providers to cease resolving DNS addresses upon request by public security departments (MII 2002; MII 2004). But perhaps most importantly, it unilaterally took the initiative to create an alternative system to handle Chinese-language domain names, which still remained globally compatible. While this system was operated relatively secretly at first, by 2006, the *People's Daily* proudly boasted that "[Chinese] Internet users don't have to surf the web via the servers under the management of the Internet Corporation for Assigned Names and Numbers of the United States" (Cited in Mueller 2012). Also, the continuing tensions over ICANN's role led the Chinese government to subsidise research on something that came to be known as IPv9: a separate technical protocol that allows systems to be "independent of the US Internet but [...] Internet compatible" (Wang and Shebzukhov 2019). Nevertheless, IPv9 seems not to play a role of any significance thus far.

New DNS regulations from 2017 illustrate the growing trend towards localisation. These regulations require entities running DNS root servers registered in China to locate their servers inside Chinese territory. Domain name registries must be based domestically, and the top-level domains these registries manage thus explicitly fall under Chinese jurisdiction. Domain name registrars equally must be Chinese entities running their systems within Chinese territory. Both registries and registrars must establish domestically-based emergency response systems and create localised backups of their databases (MIIT 2017). At the same time, there has been a certain degree of restraint. A draft version of these regulations contained a provision that "domain names with network access services within the borders" must register their domain name with a Chinese provider (MIIT 2016, Art. 37). These requirements have been

dropped in the final version, after they were widely seen as rendering all foreign websites in China unlawful. Even so, suspicions against foreign intelligence services' surveillance capabilities led to the inclusion of an article in draft regulations on data protection published in May 2019, which require that domestic Chinese Internet traffic must be exclusively routed through Chinese territory (CAC 2019). The topography of China's Internet, with only a limited number of international gateways, may facilitate the implementation of this requirement.

Data

Like governments worldwide, the Chinese leadership has become increasingly concerned about the negative effects resulting from the proliferation of online data collection and processing. In many cases, these effects are domestic, as in the case of online fraud and abuse, but the Snowden revelations also raised awareness about the potential harm from data flowing abroad. In response, Beijing started centralising its previously fragmented data protection regime, and explored the institution of strong data localisation requirements, as well as nationality requirements for data operators. Yet the exact categorisation of data to be protected, as well as the specific limitations on their export, have been subject to a to-and-fro between different regulators and stakeholders, as the need for protection is counteracted by both the economic harm from excessive limitations as well as the actual ability of government to implement and enforce data export rules.

This tension is evidenced by the tortuous development of China's regulatory framework for data protection. The drafters of the CSL intended to oblige "critical information infrastructure operators" to store both individuals' personal information and "other important data" within Chinese territory (NPC 2016). Yet the term "important data" remained undefined and was replaced with "important business data" in some intermediate drafts. Subsequent to the promulgation of the CSL, there have been successive draft data protection regulations addressing the question of data localisation and export, often going far beyond the original mandate from the CSL. 2017 draft data export regulations, for instance, not only covered critical infrastructure operators, but every "network operator", the owner of a network, a manager, and a network service provider" (CAC 2017). A subsequent draft regulation from 2019 required all network operations to conduct security assessments before exporting personal data, and to file such operations with provincial cybersecurity authorities. They also sharply curtailed data collection by foreign entities, obliging them to go through a local representative or organisation (CAC 2019A). The 2020 draft Data Security Law is largely silent on the question of cross-border data flows and localisation, containing only vague provisions that enable the government to implement export limitation measures, and which require approval for the transmission of data on request of foreign law enforcement bodies. It also explicitly established authority for China to retaliate against "any country or region that adopts discriminatory prohibitions, limitations or other such measures toward the People's Republic of China with respect to investment or trade related to data, data development and use, or technology" (NPC 2020).

Even so, none of these regulatory drafts has been adopted at the time of writing. The tortuous trajectory of data localisation over the past years illustrates the difficult

balance regulators seek to strike. There are, on the one hand, clear political and economic incentives to localise Chinese data: it is deemed to provide a defence against overseas intelligence gathering, as well as spur the development of the Chinese cloud industry. On the other hand, particularly where it comes to important data, there are considerable costs to maintaining an overly broad definition as well: enforcement resources might become spread so thin that meaningful protection is not achieved, or business is throttled through excessive red tape. With the predicted adoption of 5G and IoT technologies, these considerations will only grow in complexity.

Industrial policy

Across the board, the Chinese government has adopted industrial policy and investment measures aimed at accelerating the capacity build-up of its domestic digital industry. On the basis of highly detailed policy plans, it has developed special funding vehicles and financial support structures for the information sector, and provided the physical infrastructure it believes necessary. Domestic players receive preferential treatment in government procurement processes, and efforts in the field of digital standardisation are seen as a way to gain greater clout in the global digital space. With this support, and by leveraging the vast size of the domestic market, Chinese technology companies are now more competitive than ever with their foreign counterparts in numerous sectors, growing economic benefits while simultaneously reducing Chinese reliance on foreign technology.

In some areas, such as encryption, the use of domestic technology has been mandated for years. The Multi-Level Protection System (MLPS) for cybersecurity required high-priority networks to use domestic cybersecurity technology and cybersecurity monitoring contractors. In successive cases, Chinese authorities attempted to make domestic technology and security standards mandatory, including the encryption standards WAPI and ZUC, as well as the 3G standard TD-SCDMA. In recent years, the formulation of technology and cybersecurity standards has become more systematised. Technical Committee 260 in charge of developing cybersecurity standards, has issued over 300 separate draft standards, many of which have since taken effect. While these standards are technically not legally binding, Chinese courts and authorities nevertheless see them as best industry practices, giving them de facto a similar effect. In other cases, technical standards are incorporated into regulations by reference, vicariously making them legally binding. The extent to which foreign businesses can influence standard-setting in China is limited: a limited number of companies, including Microsoft, Cisco and Intel, were invited to join Technical Committee 260 as late as 2016. They are only allowed in five of the eight Working Groups, and barred from those addressing encryption, classified information system security, and the information security standard system. In at least one case, a standard initiative was moved from an “open” Working Group to a “closed” one after opposition by the former’s foreign members (Sacks and Li 2018).

Escalating Sino-US tensions also influenced measures aimed at mitigating vulnerability to foreign technologies. Draft measures from 2019 that create a mandatory security review process for technology used in critical infrastructure, identify both the possibility of factors such as “politics, diplomacy and trade” to disrupt the controllability, secu-

rity and supply chain integrity of products or services, as well as “situations in which product or service providers are funded, controlled, etc., by foreign governments” as priority concerns in cybersecurity reviews (CAC 2019B). Moreover, the Chinese government announced it might create an “unreliable entity list”, sanctioning foreign businesses boycotting or cutting off supplies to Chinese companies for non-commercial purposes. The Ministry of Foreign Affairs explicitly connected the actual introduction of this list with the extent to which Sino-American trade ties improved. US trade sanctions have also incentivised Chinese businesses to accelerate innovation: Huawei has prepared by developing or sourcing alternatives for technologies it might not be able to access reliably in the future, such as particular chipsets, and the Google Android operating system. As a plan B, Huawei developed HarmonyOS, a multi-platform system that might replace Android not only in smartphones, but in all kinds of connected devices. Given Huawei’s global market share, this would be a severe blow to the existing duopoly of Google and Apple.

Yet even if Chinese policymakers agree in principle on sovereignty and foreign technology, the specific way to do so is often a matter of dispute. One example is the controversy surrounding a specific Windows version for government systems. In the summer of 2017, Ni Guangnan, a member of the Chinese Academy of Engineering and a prominent advocate for the development of indigenous operating systems claimed that this version should remain outside government procurement and more broadly, that government operating systems should be “indigenous and controllable” (Ni 2017). In response, Wang Jun, General Engineer at one of the approved third party security evaluators, the CNITSEC, stated that the cybersecurity review regime does not discriminate on the basis of nationality, and that replacing Windows with an indigenous alternative would “not necessarily [be] the best choice” (Transpacifica 2017). In contrast, Wang hailed the fact that the government edition was developed by a Sino-US joint venture, in which Microsoft cooperated with CETC, with the aim of providing software that better responds to user needs and security requirements. Lastly, Wang argued that domestic operating systems might not necessarily provide a more secure alternative, merely that the risk profile might be somewhat different. This debate encapsulates many of the key points surrounding the technology substitution question in China, many of which are non-ideological or political. Some businesses, such as CETC, fare well through technological openness, others would do better if foreign competitors were absent from the market. In many cases, foreign technology is better than Chinese alternatives, and even a Huawei executive has indicated the virtuous effects of competition on innovation and security provide a strong reason to maintain openness. The existing installed base of foreign technology and integration with other systems means “rip-and-replace” might be very costly.

Lastly, central and local Chinese authorities have established various ways to facilitate businesses to obtain funding, as well as lucrative contracts and subsidies. By 2016, over 900 government-guided funds had been established, with an investment capital of USD 347 billion. As a complement to government investment, a new Science and Technology Innovation Board was set up within the Shanghai Stock Exchange, enabling fundraising among private investors. In the area of 5G, which lies at the heart of tensions between China and its major trading partners, state-owned telecommunications operator China Mobile granted over half the contracts for its 5G equipment to Huawei, and specific policy plans often indicate local content targets in various sectors and net-

work systems. Sometimes, state-run media outlets target foreign businesses in order to pressure them towards greater compliance, or to send political signals. The technology sector is no exception. In July 2019, Apple was targeted on national radio for allegedly allowing fake reviews to appear on its App Store. This compounded an already negative picture of Apple in China: Apple's smartphone share plummeted from a high of 27 per cent in 2015 to five per cent in late 2019. Huawei not only took 42 per cent of the Chinese domestic market at that time, it also had surpassed Apple as the second largest smartphone manufacturer worldwide. Partly, this may be due to political influence and nationalism among Chinese buyers, but the rapidly growing quality and feature set of Huawei's more competitively priced handsets is likely to be at least as important. Yet, the difficulties that are still facing Chinese businesses in gaining parity with their foreign counterparts should not be underestimated. China still lags behind in software and hardware components ranging from PC operating systems to semiconductors, chip manufacturing equipment to business software.

5

Conclusion

In cyberspace as well as in real space, the Chinese leadership has designated that maintaining sovereignty – supreme authority over domestic territory – is the cornerstone of its governance approach. This is largely driven by the perception of liberal values not as a universal set of values, but as a hegemonic tool in the pursuit of western powers. As such, China does not perceive liberal values as an end of history, but as an existential threat to the integrity and stability of the Chinese political system. It has sought to enshrine this in norms and agreements at the international level, and has taken considerable steps domestically to ensure sovereign capability, even in the absence of a global consensus. As China's technological development levels and sophistication have grown, it has increasingly been able to territorialise and indigenise large swathes of its digital economy and online space. Foreign suppliers, conversely, have seen their market opportunities shrink. As tensions with the United States increase, which they are likely to do, it can be expected that the impetus for a stronger assertion of sovereignty will continue to grow as well.

However, as much as the sovereignty drive has been a consequence of the increased threat from or tensions with the United States, it has also been a contributing factor. As the climate for foreign businesses has grown progressively more difficult and contentious, support for engagement with China has decreased among the corporate community, one of the relationship's key stakeholders. Furthermore, concerns about potential risks emanating from the growing global footprint of Chinese businesses has led governments across the developed world to reconsider the extent of Chinese participation in their own domestic markets. China's use of technology for domestic surveillance and control purposes, particularly in the region of Xinjiang, have exacerbated an already downward trend in perceptions of China in Europe and North America. Even without sometimes explicitly calling it so, governments are considering and taking measures in defence of their own sovereignty in ways not too dissimilar from China's approach. Huawei is facing growing difficulties to sell into Western markets, with the United Kingdom being just the latest of a series of governments that banned its participation in 5G networks. The US government is taking steps to limit the use of Chinese-owned mobile apps, most notably TikTok and WeChat. India equally banned TikTok, after border clashes with the Chinese military.

Consequently, decoupling in the digital domain has turned quickly from a policy buzzword to an incipient reality – potentially (and ironically) in a manner that may be very harmful to China. As a result of decades of comparatively borderless development, in which software, hardware and online services, their supporting business sectors and infrastructures, and flows of data and information are intertwined in complex ways. Yet from a primarily economic realm, the digital sphere has now become, for many countries, a key national security issue, ranging beyond traditional considerations such as military affairs. As the US action against TikTok demonstrates, social and even identity issues now also fall under the security umbrella. The resulting escalating trend of rapidly rising sovereign boundaries in cyberspace has the potential to change

this landscape beyond recognition. While one can only speculate as to how cyberspace might function in a decade's time, these changes will likely come at significant financial cost, and run the risk of further exacerbating the Sino-American conflict.

Europe already faces the challenge of finding its place in this bipolar reality. Regardless of whether the term sovereignty will come to be accepted as a foundational norm within the language of international law and global governance in the digital realm, current state practice de facto suggests that this is the case. Yet without countervailing efforts at maintaining some degree of co-existence, interoperability and compatibility, as well as towards generating greater trust, the price of establishing Westphalian-style sovereignty in the digital realm will be high.

This creates a quandary with regard to necessary future strategy in Europe. On the one hand, it is clear that China will not meaningfully change course or tactics with regard to the core of its economic and political digital agenda. Consequently, any influence that can be brought to bear is not going to affect more than the margins. On the other hand, cooperation with China is inevitable, and indeed necessary, both in the cyber domain as well as concerning global issues beyond – most notably climate change. Yet Europe has not been accustomed to making tough geopolitical decisions since at least the end of the Cold War, and must now learn that it cannot have it all its own way. For that reason, Europe needs to be pragmatic in its relationship with Beijing. China will follow its own trajectory, with only very limited reference to Europe's desires. Europe should thus define and prioritise its strategic interests, so its scarce political capital is spent in those areas closest to its vital interests, where progress can be made. Europe must also learn that the answer to many "China problems" lies not in Beijing, but its own capitals. Europe should take initiative on its own terms, and decide itself what it needs to safeguard and enhance its own strategic autonomy. Developing policies to achieve those goals will, however, require the mobilisation of considerable political will and resources, and is inevitably going to come at a cost.

Consequently, Europe must get its own house in order. At the multilateral level, Europe, both at the Union and individual state level, should lead through example and project itself as a successful and competent model for international rules-based governance. As a collection of small and mid-size states, it is in Europe's interest to promote a norm-based order in the digital realm, strengthening international institutions and governance structures. Where possible, this should be done with partners around the globe. It would also provide a competitive alternative to the Chinese approach that might be attractive to third countries around the world.

Lastly, it must be recognised that the China challenge is primarily an intellectual one. This has two main components. First, European decision-makers must develop a greater understanding of the geopolitical landscape that exists today. The "end of history" has – ironically – ended, and liberal democracy or market economics have not realised their universal aspirations. Certainly, the rise of China as a technological power presents many Western policymakers and business people with a reality they never imagined possible. Coming to terms with, and effectively responding to the challenges set by current circumstances cannot rely on simply reasserting old ideas, but requires a greater consideration of how these can be realistically imple-

mented in today's complex environment. Second, a greater understanding of China's worldview and functioning among European decision-makers is crucial. Thus far, levels of China-related expertise across governments and businesses are lamentable, and decisions are often made on the basis of pre-existing attitudes, speculations or extrapolations, while opportunities may be missed. This is not only important for more effective engagement with China. To be sure, a better understanding of Chinese strategic thinking, security concerns as well as the alignment of Chinese domestic stakeholders could facilitate more successful dialogue in a number of areas. Nonetheless, greater understanding does not necessarily lead to greater agreement. Yet, even outside the realm of direct bilateral relations, improved China knowledge will provide the evidentiary basis for more targeted and successful responses to China and the challenges it poses.

References

- B** Bozhkov, Nikolay. 2020. "China's Cyber Diplomacy: A Primer." EU Cyber Direct Policy Brief, accessed 22 July, 2020. https://eucyberdirect.eu/content_research/chinas-cyber-diplomacy-a-primer/.
- Broeders, Dennis, Adamsin, Liisi and Creemers, Rogier. 2019. "Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace." The Hague Program For Cyber Norms Policy Brief. November 2019.
- C** CAC. 2017. "Geren xinxi he zhongyao shuju chujing anquan pinggu banfa (zhengqiu yijian gao) (Measures for the Assessment of Personal Information and Important Data Exit Security (Draft for Soliciting Opinions))." 11 April 2017. Translation, accessed November 29, 2019. <https://chinacopyrightandmedia.wordpress.com/2017/04/11/circular-of-the-state-internet-information-office-on-the-public-consultation-on-the-measures-for-the-assessment-of-personal-information-and-important-data-exit-security-draft-for-soliciting-opinions/>.
- CAC. 2019. "Shuju anquan guanli banfa (zhenqiu yijian gao) (Data Security Management Measures (Draft for Comment))." 28 May 2019. Translation, accessed November 29, 2019. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/>.
- CAC. 2019A. "Geren xinxi chujing anquan pinggu banfa (zhengqiu yijian gao) (Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment))." June 13, 2019. Translation, accessed 29 November 2019. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/>.
- CAC. 2019B. "Wangluo anquan shencha banfa (zhenqiu yijian gao) (Cybersecurity Review Measures (Draft for Comment))." 21 May 2019. Translation, accessed November 29, 2019. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-critical-systems-add-focus-supply-chain-foreign-control-translation/>.
- G** Griffiths, James. "The Great Firewall of China: How to Build and Control an Alternative Version of the Internet." London: Zed Books 2019.
- H** Houser, Kimberly A. 2020. "The Innovation Winter Is Coming: How the U.S.-China Trade War Endangers the World." San Diego Law Review. 57 (3). accessed 18 November 2020. <https://digital.sandiego.edu/cgi/viewcontent.cgi?article=3383&context=sdlr>.
- Hu, Jintao. 2011. "Jianding buyi zou Zhongguo tese shehuizhuyi wenhua fazhan daolu: nuli jianshe shehuizhuyi wenhua qianguo (Resolutely Walk the Path of Socialist Culture Development with Chinese Characteristics: Striving to Construct a Strong Socialist Culture Country)." Qiushi. Translation, accessed 28 November 2019. <https://chinacopyrightandmedia.wordpress.com/2012/01/04/hu-jintaos-article-in-qiushi-magazine-translated/>.


- J** Jiguang. S. d. "Jiguang dashuju: 2017 nian yidong hulianwang hangye panduan app bangdan (Jiguang data: a 2017 list of apps in the mobile Internet sector)." Accessed 29 November 2019. <https://www.jiguang.cn/reports/195>.
- K** Kent, Ann. 2008. "China's Changing Attitude to the Norms of International Law and Its Global Impact." In *China's "New" Diplomacy*, edited by Kerr, Pauline, Stuart Harris and Yaqing Qin, 55–76. New York: Palgrave Macmillan.
- Klimburg, Alexander. 2013. "The Internet Yalta." Center for a New American Security. Accessed 29 November 2019. http://dragon-report.com/Dragon_Report/home/home_files/The%20Internet%20Yalta.pdf.
- L** Lu, Wei. 2013. "Wang ju zhengnengliang, gong zhu Zhongguo meng: zai di shisan jie Zhongguo wangluo meiti luntan shang de zhuzhi yanjiang (Concentrate Positive Online Energy, Jointly Build the Chinese Dream: Speech at the 13th China Online Media Forum)." 30 October 2013. Translation, accessed 29 November 2019. <https://chinacopyrightandmedia.wordpress.com/2013/10/30/siio-director-outlines-eight-objectives-for-online-media/>.
- M** MFA. 2017. "Wangluo kongjian guoji hezuo zhanlüe (International Strategy of Cooperation on Cyberspace)." 3 January 2017. Translation, accessed 22 November 2019. <https://chinacopyrightandmedia.wordpress.com/2017/03/01/international-strategy-of-cooperation-on-cyberspace/>.
- MFA. 2019. "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security." Accessed 29 November 2019. <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-owwg-en.pdf>.
- MII. 2002. "Zhongguo hulianwangluo yuming guanli banfa (Management Rules for Domain Names on the Chinese Internet)." 1 August 2002. Accessed 29 November 2019. <http://www.people.com.cn/GB/14677/21980/22078/1898076.html>.
- MII. 2004. "Zhongguo hulianwangluo yuming guanli banfa (Management Rules for Domain Names on the Chinese Internet)." November 5, 2004. Accessed 29 November 2019. <http://www.miit.gov.cn/n1146295/n1146592/n1146754/n1234736/n1234739/n1234740/c3099778/content.html>.
- MIIT. 2016. "Hulianwang yuming guanli banfa (xiuding zhengqiu yijian gao) (Internet Domain Name Management Rules (Opinion-seeking Revision Draft))." 25 March 2016. Translation, accessed 29 November 2019. <https://chinacopyrightandmedia.wordpress.com/2016/03/25/internet-domain-name-management-rules-opinion-seeking-revision-draft/>.
- MIIT. 2017. "Hulianwang yuming guanli banfa (Internet Domain Name Management Regulations)." 16 August 2017. Accessed 29 November 2019. <https://baike.baidu.com/item/互联网域名管理办法/23443734?fromtitle=中国互联网络域名管理办法&fromid=1778530>.

- Mueller, Milton. 2012. "China and Global Internet Governance: A Tiger by the Tail." In *Access Contested: Security, Identity and Resistance in Asian Cyberspace*, edited by Deibert, Ronald, 177–94. Cambridge: MIT Press.
- N** Ni, Guangnan, 2017A. "Zhengfu caozuo xitong ying quebao zizhu kekong (Government Operating Systems Should Be Guaranteed Indigenous and Controllable)." *Global Times*. 13 June 2007. Accessed 29 November 2019. <https://opinion.huanqiu.com/article/9CaKrK3qF3>.
- NPC. 2016. "Zhonghua renmin gongheguo wangluo anquan fa (Cybersecurity Law of the People's Republic of China)." 7 November 2016. Translation, accessed 22 November 2019. <https://chinacopyrightandmedia.wordpress.com/2016/11/07/cybersecurity-law-of-the-peoples-republic-of-china/>.
- NPC. 2020. "Zhonghua renmin gongheguo shuju anquan fa (cao'an) (Data Security Law of the People's Republic of China (Draft))." 1 July 2020. Translation, accessed 22 July 2020. <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/>.
- Q** Qiushi. 2013. "Yike ye buneng fangsong he xueruo yishixingtai gongzuo, renzhen xuexi guanche quanguo xuanchuan sixiang gongzuo huiyi jingshen (We Cannot Slacken or Weaken in Ideological Work Even for One Moment – Earnestly Study and Implement the Spirit of the National Propaganda and Ideology Work Conference)." *Qiushi*. Translation, accessed 22 July 2020. <https://chinacopyrightandmedia.wordpress.com/2013/09/01/we-cannot-slacken-or-weaken-in-ideological-work-even-for-one-moment-earnestly-study-and-implement-the-spirit-of-the-national-propaganda-and-ideology-work-conference/>.
- S** Sacks, Samm and Li, Manyi Kathy. 2018. "How Chinese Cybersecurity Standards Impact Doing Business in China." CSIS Briefs. Accessed 29 November 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF.
- SCIO. 2010. "The Internet in China (White Paper)." 8 June 2010. Accessed 22 October 2019. http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.
- Schell, Orville and Delury, John. 2014. *Wealth and Power: China's Long March to the Twenty-First Century*. New York: Random House, 2014.
- T** TransPacifica. 2017. "Chinese IT Security Examiner Describes Review Process, Clarifies Status of Chinese Government Windows Edition." Accessed 29 November 2019. <http://transpacifica.net/2017/06/1963/>.
- W** Wang, Yubian and Shebzukhov, Yuri. 2019. "From Network Security to Network Autonomous." *International Journal of Advanced Network, Monitoring and Controls* 4(1). 61–5.
- X** Xue, Hong. 2004. "Voice of China: A Story of Chinese-Character Domain Names." *Cardozo Journal of International and Comparative Law* 12. 559–92.

- Z Zhang, Weiwei. 2013. "Cong guoji zhengzhi shijian kan 'pushi jiazhi' de duozhong kunjing (Looking at the Multiple Difficulties of "Universal Rights" from International Political Practice)." Qiushi. Translation, accessed 22 July 2020, <https://chinacopy-rightandmedia.wordpress.com/2013/10/16/looking-at-the-multiple-difficulties-of-universal-rights-from-international-political-practice/>.

Author

Rogier Creemers is Assistant Professor at Leiden Institute for Area Studies, Leiden University. He combines degrees in Chinese Studies, International Relations and Law. His research explores how the Chinese Communist Party views its role in governance, and uses technology to further its project. With a VIDI grant from the Netherlands Organisation for Scientific Research, he leads a project to chart the development of a tech-enabled “smart state” in China.



In this paper, Rogier Creemers explains the foundations of Chinese digital policy in the 21st century along the lines of the concept of cyber sovereignty. In order for Europe to assert its interest and values while China rises as a digital power, it is essential to analyze and comprehend the People's Republic's approach towards the digital realm.