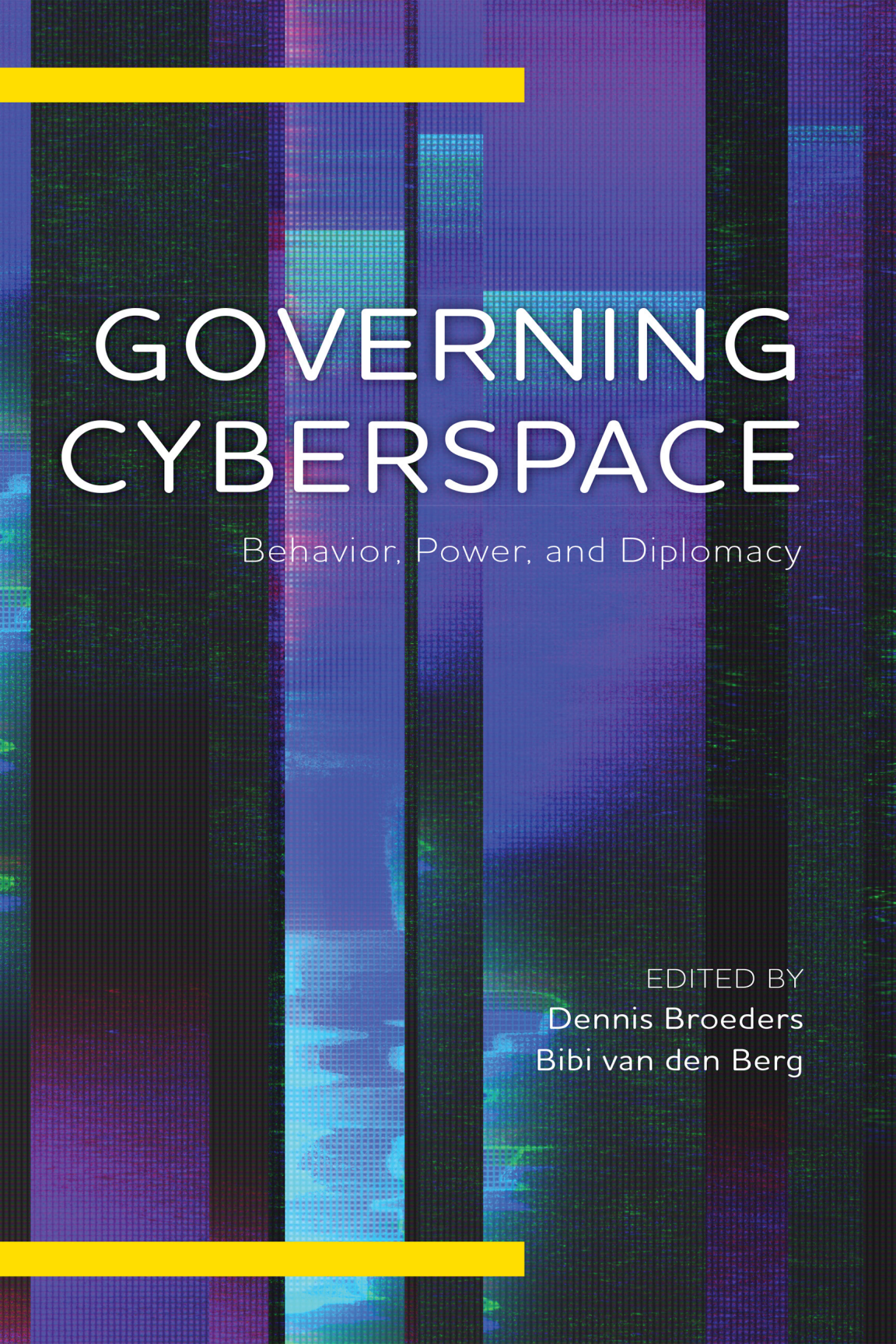
China's conception of cyber sovereignty: rhetoric and realization

Creemers, R.J.E.H.; Broeders, D.; Berg, B. van den


GOVERNING
CYBERSPACE
Behavior, Power, and Diplomacy
EDITED BY
Dennis Broeders
Bibi van den Berg

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.

Digital Technologies and Global Politics

Series Editors: Andrea Calderaro and Madeline Carr

While other disciplines like law, sociology, and computer science have engaged closely with the Information Age, international relations scholars have yet to bring the full analytic power of their discipline to developing our understanding of what new digital technologies mean for concepts like war, peace, security, cooperation, human rights, equity, and power. This series brings together the latest research from international relations scholars—particularly those working across disciplines—to challenge and extend our understanding of world politics in the Information Age.

Governing Cyberspace: Behavior, Power, and Diplomacy, edited by Dennis Broeders and Bibi van den Berg

Governing Cyberspace

Behavior, Power, and Diplomacy

Edited by
Dennis Broeders
Bibi van den Berg

ROWMAN & LITTLEFIELD
Lanham • Boulder • New York • London

Published by Rowman & Littlefield
An imprint of The Rowman & Littlefield Publishing Group, Inc.
4501 Forbes Boulevard, Suite 200, Lanham, Maryland 20706
www.rowman.com

6 Tinworth Street, London, SE11 5AL, United Kingdom

British Library Cataloguing in Publication Information Available

Library of Congress Cataloging-in-Publication Data

Names: Broeders, D. (Dennis), editor. | Berg, Bibi van den, editor.
Title: Governing cyberspace : behavior, power, and diplomacy / edited by Dennis Broeders, Bibi van den Berg.
Description: Lanham : Rowman & Littlefield, [2020] | Series: Digital technologies and global politics | Includes bibliographical references and index. | Summary: "Contributes to the discussion of growing insecurity and the unpredictable and often authoritarian use of the digital ecosystem"—Provided by publisher.
Identifiers: LCCN 2020004795 (print) | LCCN 2020004796 (ebook) | ISBN 9781786614940 (cloth) | ISBN 9781786614957 (paperback) | ISBN 9781786614964 (epub)
Subjects: LCSH: Computer networks—Law and legislation. | Internet—Law and legislation. | Cyberspace.
Classification: LCC K564.C6 G685 2020 (print) | LCC K564.C6 (ebook) | DDC 343.09/944—dc23
LC record available at https://lccn.loc.gov/2020004795
LC ebook record available at https://lccn.loc.gov/2020004796

 The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI/NISO Z39.48-1992.

Contents

Acknowledgments

This book resulted from the inaugural conference of the Hague Program for Cyber Norms, titled "Novel Horizons: Responsible Behaviour in Cyberspace," which was held in the Hague on November 5–7, 2018. The editors thank the participants for a great conference and especially those that submitted their work for this edited volume.

A first round of editorial comments was done for the conference itself, and we thank Liisi Adamson, Els de Busser, Ilina Georgieva, and Zine Homburger, who were at the time all affiliated to the program, for their editorial contribution. We also thank Corianne Oosterbaan for all her hard work organizing the conference and her invaluable help with the editorial process.

Lastly, we would like to thank the Dutch Ministry of Foreign Affairs who generously fund the Hague Program for Cyber Norms and all of its activities and publications.

The Hague, 2.12.2019
Dennis Broeders and Bibi van den Berg

Chapter 6

China's Conception of Cyber Sovereignty

Rhetoric and Realization

Rogier Creemers[1]

INTRODUCTION

Since its initial connection to the global Internet in the 1990s, China has experienced a tremendous technological leap forward. Over 850 million Chinese individuals have become network users (CNNIC 2019), using increasingly sophisticated devices to access a rapidly burgeoning digital economy. Chinese hardware and software businesses, including Alibaba, Tencent, Huawei, and ZTE, have become industry leaders with a growing global footprint. Technology questions have swiftly gained political prominence, reflected in the creation and expansion of institutions such as the Cyberspace Administration of China (CAC) and the Central Commission for Cybersecurity and Informatization, chaired by Xi Jinping personally (Creemers 2019). Yet, the nomenclature of the latter body also points at a tension fundamental to China's technology policy: while informatization—the introduction of information technologies (ITs) into social and economic life—promises considerable benefits, it equally creates considerable security concerns.

These concerns are not limited to technical questions surrounding the integrity, availability, and correct functioning of IT systems and the data stored within them. For decades, the Chinese leadership has feared ideological subversion, and has designated online content as a potential weapon for "peaceful evolution" (Wang 2011). In recent years, the growing adoption of ITs and tensions resulting from China's expanding geopolitical role have led to new worries, particularly in relation to the United States. Overall, China sees itself standing at the wrong end of a digital divide, where the distribution of resources and capabilities in cyberspace is highly asymmetric

(Shen 2016). The Snowden revelations, US technology export bans targeting ZTE and Huawei, and the discontinuation of security support for Windows XP each highlighted vulnerabilities resulting from forced reliance on currently irreplaceable US technology. Until its reform process, the Internet Corporation for Assigned Names and Numbers (ICANN) was often viewed as an extension of the US government. US-led efforts to curtail the global presence of Huawei, particularly its participation in the standardization process for fifth-generation mobile networks (5G) form one of the major elements of what some observers already call the "US-China technology cold war" (Yuan 2019). Concerns about surveillance and espionage, the survival of national economic champions and even China's basic ability to access the global Internet thus joined propaganda and ideology in Chinese technology policy.

Inasmuch as the tensions between China and the United States (or more broadly, the "like-minded" nations) result from competing national interests, they are also the product of opposed views on the role of IT in the relationship between the state, citizens, and the economy. Since the 1990s, the U.S. tech community has espoused a "free and open" view of the Internet, embodying American liberal democratic norms including free speech, access to information and free-market capitalism, as well as some of the libertarian ethics of the academic and engineering communities that created the Internet. The economic dominance of the US tech industry, and the central role played by these communities, meant these views were nearly universally disseminated without much opposition as the Internet expanded in the decades since (Demchak 2016). Over the past decade, however, China has become increasingly vocal and active in defending a different approach, one based on "cyber sovereignty" (*wangluo zhuquan*).

Cyber sovereignty has become a mainstay in documents and statements for international consumption since its first high-profile appearance in the 2010 White Paper outlining China's position on the Internet (SCIO 2010). Together with Russia, China proposed a Code of Conduct for state behavior in the United Nations General Assembly in 2011 (UN 2011) and again in 2015 (UN 2015). Sovereignty was the first of five principles for international cooperation in cyberspace that the Chinese delegation proposed at the 2012 Budapest Conference on Cyberspace (MFA 2012), and the second item in the Wuzhen Declaration that China proposed at the first World Internet Conference in 2014 (WIC 2014). It has been a repeated element in speeches by top leaders including General Secretary Xi Jinping (Xi 2015) and ex-Internet "czar" Lu Wei (Lu 2014), as well as a key objective in China's national cybersecurity strategy (CAC 2016a), its Cybersecurity Law (NPC 2016C), its development program for the ICT sector (Central Committee and State Council 2016), and its international cyber strategy (MFA 2017).

These policy documents usually define cyber sovereignty in vague and broad terms. In the words of Xi Jinping, a state has the right "to choose its online development path, its network management model and its public Internet policies, and to equal participation in international cyberspace governance." In turn, states should refrain from "engaging in cyber hegemony, interfering in other countries' internal affairs, and engaging in, tolerating or supporting online activities harming the national security of other countries" (Xi 2015). Yet, what this implies in specific national and international legal, regulatory and policy questions is often unclear, and subject to considerable debate in China itself (Zeng, Stevens and Chen 2017). Existing literature has primarily focused on the discussion of sovereignty in diplomatic processes and foreign policy, such as global Internet governance regimes including ICANN, WSIS, and the Internet Governance Forum (Shen Hong 2016; Mueller 2012; Arsène 2012), military and strategic cybersecurity (Swaine 2013; Harold, Libicky and Stuth Cevallos 2016; Kolton 2017; Lindsay 2014), and the reshaping of the global cyber order (Demchak 2016). However, in this literature, cyber sovereignty is largely taken as given, and the substance of the concept, as well as its role as an organizing principle for cyberspace, receives little attention. This chapter thus intends to bookend this body of literature by supplementing two elements: first, how the cyber sovereignty concept emerges as part of China's broader approach to foreign policy, and second, how Chinese authorities have structured the domestic legal, regulatory, and policy landscape in order to realize the goals sovereignty entails.

This chapter contains two sections. The first section explores the development of China's conception of sovereignty, both general and cyber-related, against a historical background. It will pay particular attention to how China's reading of sovereignty embodies its broader views of the global order, as well as to the multidimensional nature of the sovereignty concept. It will identify two major components of the sovereignty concept: a normative component defining how states should conduct themselves in cyberspace, and a capability component that identifies the governance and material resources and mechanisms a state requires to realize the normative component in a potentially antagonistic environment. The second section will review how China has sought to construct these governance and material resources through law, regulation, and policy. It finds the Chinese state has mainly sought to institute and consolidate effective control over online actors, activities, and content through a process of territorialization, indigenization, and investment, while maintaining technical interoperability with the global Internet. Even so, there is a considerable degree of complexity: although it is one thing to declare cyber sovereignty, it is quite another thing to unpick the tightly woven fabric of the digital society without undue harm, particularly as the interests of

various Chinese stakeholders are often at odds. The conclusion will discuss practical and theoretical implications of these processes for the global Internet.

THE CONCEPT OF SOVEREIGNTY IN CYBERSPACE

Parallel Histories

While the classical attribution of sovereignty to the 1648 Peace of Westphalia has been disputed, it is generally accepted that the notion of sovereignty—supreme and exclusive political authority within a bounded territory—was consolidated across Europe in the seventeenth century. This international order was based on the principles of non-intervention and sovereign equality: no foreign entity outranked the ruler of a territory, or was permitted to interfere in its internal affairs (Krasner 1999). This was particularly important with regard to religion. Religious wars had wrought havoc across the continent for over a century. In this sense, with the principle of *cuius region*, *eius religio*, sovereignty expressed an agreement to disagree: disputes over alleged universal moral truths would no longer form a justification for conflict. In the centuries since, the sovereign state has become the primary form of territorial organization worldwide.

To be sure, the sovereignty principle has often been honored in the breach as much as the observance. The attempted invasion by monarchical powers into revolutionary France, for instance, was largely justified by arguments for regime change. Racist ideas concerning "civilization" withheld sovereignty from much of the non-European world until after World War II. Yet, as decolonizing states increasingly achieved sovereignty and self-determination, another trend toward constraining sovereignty started gaining traction: one to limit state cruelty and injustice. In the wake of the Holocaust, the Universal Declaration on Human Rights became the first component of a growing body of human rights law. The Helsinki Process of the 1970s created commitments on civil rights that greatly encouraged dissident and democratic movements in the USSR and its satellite states (Thomas 2001). Following the end of the Cold War, doctrines such as the Responsibility to Protect further eroded the authority of the non-intervention norm (Glanville 2013). Lastly, *de facto* if not *de jure*, economic globalization has grown to considerably curtail the space for movement of states, and consolidated the dominance of a (neo-) liberal capitalist model around the world (Stein 2016).

China's approach to sovereignty, in contrast, was predominantly concerned with a drive to counteract the presence of imperialist powers that had established extraterritorial rule in their concessions and had taken over a number of Chinese government authorities, and start China on a path back toward

wealth and strength (Schell and Delury 2014). Their efforts rarely met with success. At the end of World War I, China hoped to cash its material support for the allies with the return of German-held concessions in Shandong. Delegation member (and later International Court of Justice judge) Wellington Koo eloquently argued that the Wilsonian principles of independence and self-determination implied Japan's competing claims should be rejected. The territories were subsequently handed over to Japan as part of a compromise to mitigate tensions in the Pacific and stave off Japanese calls for the explicit recognition of racial equality in the League of Nations (MacMillan 2011, chapters 23–24). In China, this disappointment triggered dejection, protests, a transformational nationalist cultural movement (Forster 2018), the establishment of the Chinese Communist Party, and a lingering sense that, in the final analysis, foreign powers were not serious in their stated commitment to international law, but would use it as an instrument of power (Kent 2008). China's task, therefore, would be to acquire power, not play the law game.

Distrust continued to color the foreign relations of the Chinese Republic and People's Republic, even with its nominal allies. During World War II, even though Chiang Kai-shek managed to secure agreements ending extraterritoriality and renouncing territorial concessions from Britain and the United States, the alliance was strained due to Chiang's—not unjustified—sense that both countries were only doing the bare minimum to keep China in the war and Japanese soldiers tied up (Mitter 2013). Ideological differences, disagreements on relationships with the West, and competition for leadership in the global Communist movement led Mao to curtail relationships with the Soviet Union in the early 1960s. China's near-total isolation from global diplomacy would last until the 1970s, when gradual overtures toward the United States led to Beijing's takeover of the Chinese membership of the UN, hitherto held by Taipei, and the recognition of the People's Republic by most nations worldwide. The Dengist reforms further spurred openness to the outside world, as China started participating in numerous global diplomatic and legal regimes. Yet, even as China developed a more pragmatic form of global engagement, the rhetorical basis of China's foreign policy remained the Five Principles of Peaceful Coexistence, developed in the mid-1950s, of which sovereignty was the most important one (Kent 2008).

The Tiananmen events of 1989 underscored the distance the regime would go to, to safeguard its existence, and in a certain sense, their aftermath has continued to shape China's relationship with the outside world. Coinciding with the end of Communist regimes in Eastern Europe and the dissolution of the Soviet Union, the West came to believe that Tiananmen indicated it would only be a matter of time until the Chinese regime would follow them into the annals of history (Pei 2006; Chang 2010). Human rights became an important part of American and European diplomatic efforts toward China,

and democratization became one of the key themes of China scholarship. The Chinese leadership, however, considered its response to the Tiananmen protests as a regrettable but necessary defensive measure. Since then, stability maintenance (*weiwen*) has been one of the cornerstones of Chinese domestic politics, affecting areas ranging from media and education to policing and surveillance (Wang and Minzner 2015). The explicit Western support for the Tiananmen protests, as well as liberal activism in the decades since, has fostered further distrust among the leadership about Western intentions vis-à-vis China. Senior leaders and party media often refer to the efforts by "foreign hostile powers" (Hu 2011) that attempt to Westernize and divide China, or subvert CCP leadership. China's conception of sovereignty embodies the core of these tensions: China's definition of sovereignty primarily concerns the integrity of its political structure, while Western states consider this a defence of exactly those abuses that the more conditional, post–Cold War reading of sovereignty sought to curtail.

Sovereignty and Cyberspace

The controversy concerning cyber sovereignty is one specific manifestation of these broader tensions. Here as well, China's views of the role of the state evolved separate from those in the West, where the trend has been one of progressive withdrawal of the state. For the first few decades of their development, information technologies were primarily driven by national security interests, and more specifically, intelligence, surveillance, and encryption (Corera 2015), as well as prestige projects such as Apollo. However, the growing adoption of computers by businesses and individuals meant that states gradually lost their exclusive control over networking and encryption technologies. In the United States, a budding community of academics and engineers started building what became the Internet, on the basis of libertarian ethical principles of openness, transparency, and skepticism of government. Governments attempted to resist their efforts for a while, during the crypto wars of the 1980s. But the relaxed political environment following the end of the Cold War encouraged the broad adoption of this mind-set, including by governments. No longer a secretive part of the state's security arsenal, information technology came to symbolize the post–Cold War belief that liberal democracy and free-market capitalism were the inevitable end of history (Demchak 2016).

In this techno-optimist view, cyberspace had become a phenomenon all of its own, in which traditional government no longer played a significant role. John Perry Barlow's Declaration of the Independence of Cyberspace explicitly claimed that governments, "weary giants of flesh and steel," no longer had sovereignty in the digital domain (Morrison 2019). Technology businesses

enthusiastically embraced this narrative of openness, with its rejection of strong government regulation, as it allowed them to rapidly grow on a global scale. Political and economic elites came to see digital technology as a solution for a wide variety of economic and social ills, but also as a battering ram against the remaining bastions of authoritarianism. The reduced role of the state also became clear in many aspects of Internet governance, for instance, in ICANN and the Internet Engineering Task Force (IETF), where the multistakeholder model became the norm (Dutton and Peltu 2008). In this model, technical and business communities, as well as civil society, became at least as important as government in creating governance rules for the Internet.

China's relative latecomer status to information technologies meant it had little influence or participation in the emergence of these processes. Nonetheless, it espoused its own version of techno-optimism, which led it to espouse information technologies enthusiastically with its agenda of "informatization" (*xinxihua*) (Qu 2010). This optimistic view shared the basic principle that digital technology could address socioeconomic questions, but fundamentally disagreed with its liberal democratic precepts. Rather, technologies were marshalled as part of the broader CCP project that sought to combine economic development with strict political control, under the exclusive authority of the party (Central Committee and State Council 2016). Related tactics the party employed elsewhere were extended into the sphere of technologies, including media control and limitations to foreign and private participation in strategic economic sectors. By design, these tactics limited both commercial opportunities for foreign players, and the political liberalization foreign observers hoped for, leading to growing criticism. It is in response to this criticism, as well as the growing prominence of cyber-related questions in the diplomatic realm, that the concept of cyber sovereignty entered the political jargon.

In 2010, the Chinese government published its first comprehensive justification of its approach to cyberspace governance. This White Paper stated that, as the Internet fell under the jurisdiction of Chinese sovereignty, everyone within Chinese territory was obliged to obey Chinese laws and regulations (SCIO 2010). In 2012, at the Budapest Conference on Cyber Issues, China proposed five principles for international cooperation on cyberspace, echoing the Five Principles of Peaceful Coexistence. Sovereignty was the first of these, defined as the entitlement of every state to "formulate its policies and laws in light of its history, traditions, culture, language and customs (MFA 2012)." At that point in time, the chief matter of concern was online content. Subsequent policy documents have slightly expanded on these principles, or were updated to reflect new concerns. The Wuzhen Declaration, circulated at the first World Internet Conference in 2014, stated that "We should respect each country's rights to the development, use and governance of the Internet, refrain from abusing resources and technological strengths to violate

other countries' Internet sovereignty" (WIC 2014). Xi Jinping reiterated this stance in his Wuzhen speech the following year (XI 2015). The 2016 National Cyberspace Security Strategy explicitly defended states' rights to "prevent, curb and punish the online dissemination of harmful information endangering national security and interests, and to safeguard order in cyberspace" (CAC 2016a). The most elaborate discussion of sovereignty in a policy document can be found in the 2017 International Strategy of Cooperation on Cyberspace, and deserves to be quoted in full.

> 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)

China's Concept of Cyber Sovereignty: The Normative Dimension

The above descriptions, however vague, do allow the abstraction of three implicit general principles underpinning the cyber sovereignty concept. The first principle is that national governments enjoy sovereign rights against other national governments. This principle primarily is a response against the universalist claims of the proponents of online openness. By reserving the right to control all online activities under their jurisdiction to national governments, this principle rejects the applicability of universal rights, including

free expression and access to information, as well as potential moves by adversaries to realize those rights, for instance, through circumvention software. It is also up to individual states to decide how to use technology for purposes such as domestic surveillance and law enforcement. At a secondary level, it defends the right of states to organize and develop their digital industries as they see fit. This can entail development strategies including state subsidies and other forms of support, but also market access and security review regimes for foreign software and hardware, as discussed below.

The second principle is that national governments enjoy sovereignty over all non-state actors, be they domestic or foreign. This principle opposes the multistakeholder model of Internet governance that had been developed through institutions such as ICANN and the IETF, and endorsed by WSIS and the IGF. Instead, even if the technical and commercial communities have an important role to play, final authority should be exercised by nation-states through intergovernmental institutions. China's call for transforming ICANN into a specialized UN body under the ITU is perhaps the most prominent manifestation of this principle. Nonetheless, China has also come to propose a "multi-party" model, in which the consultative role of non-state entities is explicitly recognized. The importance of this model should not be overstated. China's Internet ecology consists of numerous industry associations and professional bodies that fall under the formal authority of state ministries, or whose senior officials are appointed by the CCP. Business leaders, too, are often party members. While that does not mean monolithic acceptance of central state policy—often quite the opposite—this model combines a semblance of institutional pluralism while maintaining a considerable degree of political control.

The third principle is sovereign equality of states in Internet governance. Under this principle, no state should have more power than others, or seek hegemony. This principle clearly targets what China sees as the hegemonic position of the United States, but it also has important tactical considerations in the multilateral context. As evidenced by the high level of support for the reforms Russia and China proposed in the ITU meeting of 2012 (Klimberg 2013), as well as for the Open-Ended Working Group on norms for state behavior in cyberspace at the 2018 UN General Assembly, a significant number of countries worldwide at least partially share China's position. In other words, the sovereignty narrative is also attractive to small and midsize player with whom China might seek common cause.

China's Concept of Cyber Sovereignty: The Capability Dimension

The three abovementioned normative principles undergird China's diplomatic efforts, but have also inspired an ongoing expansion of domestic measures

to ensuring sovereignty can be realized for China itself, even in the absence of international adoption. These measures have converged around three core strategies: territorialization, indigenization, and investment.

Territorial boundaries are a key component of the concept of sovereignty, but have been largely anathema in discussions on cyberspace. From a technical perspective, geography plays no meaningful role in the functioning of the Internet, even if the underlying infrastructure is territorial, and the absence of online borders was key to the techno-optimist view of cyberspace as a completely *sui generis* creature. Unsurprisingly, the Chinese government has taken a rather different approach. In 2013, CAC director Lu Wei stated that cyberspace is an extension of real space, and that it is, therefore, not a "land outside the law" (*fa wai zhi di*, Lu 2013). Yet, claiming jurisdiction over cyberspace implies having to define its limits and instituting border controls. Partly, the Chinese government has been able to do so through physical infrastructure: the Great Firewall's hardware is mainly located at China's international gateways (Lee 2018). But territorialization can also take place through regulatory means: by mandating that particular actors, activities, and data are located within China, jurisdictional questions are avoided altogether.

The indigenization strategy intends to increase the proportion of technology used in Chinese cyberspace that is produced by Chinese suppliers. For most of the 2000s, the vast majority of information technology products used in China originated from foreign businesses, from Cisco routers in the network infrastructure to Microsoft operating systems, from Apple smartphones and laptops to domain names purchased from foreign registrars. In 2014, a party journal claimed that 82 percent of servers, 73.9 percent of storage equipment, 95.6 percent of operating systems and 91.7 percent of databases in the country were foreign-sourced (Zhao and Xu 2014). A number of events highlighted China's vulnerability to both foreign corporate decisions and governmental acts. When Microsoft announced in early 2014 that it would no longer support Windows XP, for instance, this operating system was still in use in the majority of Chinese computers. In response, China banned Windows 8 from government systems (Kai 2014), and Microsoft reversed its position. The Snowden revelations generated widespread concern about the possible implantation of backdoors or other forms of malicious code into foreign ICT equipment (Xi 2013, *People's Daily* 2014). For both economic and political reasons, the Chinese government has increasingly sought to substitute foreign suppliers by domestic counterparts across a range of sectors. As a result, foreign content providers and online platforms have either not gained a significant foothold on the Chinese market, or in the case of Google, ended their Chinese activities as they were unwilling to comply with government demands. The four brands Huawei, Oppo, Vivo, and Xiaomi combined now hold over 80 percent of China's market share. China has also attempted

to develop indigenous technological standards and stimulated its domestic businesses to participate in the formulation of global standards, most notably 5G. The success of this indigenization strategy nevertheless remains uneven. In many areas, including operating systems and semiconductors, Chinese products lag far behind foreign counterparts in quality, security, and market success (Triolo 2019). Equally, the international adoption of Chinese standards, as well as Chinese participation in global standards, remains extremely limited.

To remedy these weaknesses, the Chinese government has deployed several industrial policy schemes across the technological spectrum. One major destination of funding has been research and education, both for general purposes and specific technical capabilities. Universities have been encouraged to expand computer science and cybersecurity curricula, expanding China's talent pool, with an increasing focus on emerging technologies such as big data and artificial intelligence (State Council 2016). Support is also offered through favorable government procurement policies or direct subsidies under industrial plans such as Made in China 2015 and the Internet Plus plan (Wübbeke et al. 2016). The Digital Silk Road component of the Belt-Road Initiative supports Chinese technology businesses in their international development (Shen 2018). Some of these strategies have, however, backfired. For instance, governmental guidance funds meant to provide venture capital for the technology sector have been less successful than intended (Feng 2018). Moreover, governmental support for China's technology businesses is a major factor driving the worsening of relations with major trading partners.

REALIZING SOVEREIGNTY AT HOME

The Chinese government has used various combinations of these three strategies in order to realize its cyber sovereignty objectives, going back to the early 2000s in some cases. This process has intensified since 2013, for a number of contributory reasons. Some of these concern the rapidly expanding adoption and complexity of ITs in general. From the point of view of sovereignty, they can also be seen as a response to two trends at the international level. First, China's sovereignty stance has found little traction in existing cyber governance circles thus far. Partly, this is due to symbolic reasons. "Like-minded" governments have come to see sovereignty as a shibboleth to justify of authoritarianism. Consequently, even if many of them have come to favor a somewhat greater degree of governmental control, they have been hesitant to endorse the inclusion of national sovereignty. On the Chinese side, this has stimulated accusations of hypocrisy. Chinese commentators have argued that initiatives such as the US buildup

of military cyber capabilities, and the introduction of the EU General Data Protection Regulation, are expressions of sovereign power in cyber affairs. Second, the likelihood of any agreement has become more remote as the Sino-American relationship has sharply deteriorated, most prominently through tensions concerning digital technology. During the second term of the Obama administration, the United States stepped up pressure against China on issues concerning cyber espionage, leading to an agreement in 2015 that neither state would conduct or condone such activities (Sevastopulo and Dyer 2015). The advent of the nationalist Trump administration, which campaigned on a strong anti-China platform, and growing disillusion about the treatment of American businesses severely weakened the stabilizing role of the trade component in the overall relationship. As part of a broader trade war, the US government launched an investigation concerning Chinese technology transfer requirements and intellectual property infringement, finding these constituted unreasonable burdens to US businesses (Congressional Research Service 2018). It also imposed sanctions against ZTE and Huawei for the violation of sanctions against Iran (SCMP 2018). Reversing decades of economic integration, "decoupling" became a buzzword both in Washington and Beijing, particularly in the tech sector (Panda 2019). These evolutions fostered a greater sense of urgency in Beijing to enhance resilience, autonomy, and self-reliance (*zili gengsheng*, Thomas 2019), while still maintaining the advantages of global connectivity and interoperability. This section will review how this balance has been pursued in the areas of content control, the Domain Name System (DNS), data protection, and the engagement with foreign digital corporations.

Content Control

Perhaps the best-known boundary in cyberspace is the Great Firewall of China, the filtering infrastructure at the international gateways of China's telecommunications networks that filters out undesirable content. Established in the late 1990s, it has been upgraded of the years to effectively remove from Chinese audiences content produced outside of Beijing's ability to control. This includes explicitly political content, such as websites defending Falun Gong, the Tibetan or Uyghur cause, online media outlets reporting critically in China, social media networks that had been implicated in political events such as the Arab Spring and color revolutions in ex-Soviet states, as well as morally undesirable content such as pornography (Griffiths 2019). Allegedly, it was used to leverage the "Great Cannon" attack, which targeted developer platform GitHub in 2015 (Marczak et al. 2015). The Great Firewall has also been periodically updated to target circumvention software. For instance, particular commercial VPN services work less effectively around major national

celebrations, and The Onion Router (TOR), which enables anonymous and encrypted web access, does not function reliably from China.

Yet, the Great Firewall is not the only barrier to foreign content. Starting in 2000, authorities started expanding the previous regulatory regime for media from the traditional realm to the Internet. The first provisional regulations already contained a ban on foreign audiovisual content on Chinese websites (SARFT 2000, Art. 16[g]), and imposed licensing requirements for online operators. The permitted share of foreign participants in online information services' joint ventures was limited (State Council 2000, Art. 17), while the Chinese WTO accession schedule limited foreign market access for many media-related activities (MOFCOM 2001). Subsequent regulations barred foreign participation from activities such as news (SCIO and MII 2005, Art. 9), online publishing (CAC 2016b, Art. 10), and provision of audiovisual content (SARFT 2004, Art. 7). Unsurprisingly, these regulatory barriers, in combination with a protectionist stance in favor of Chinese businesses, meant no large foreign online operator has been able to maintain a sustained presence on Chinese territory. Google had set up operations in Beijing in 2005 but closed down its Chinese search engine in 2010 after it discovered state-backed hacking operations into its user data (Waddell 2016). More recently, Facebook attempted to open a start-up incubator subsidiary in Hangzhou, but after a miscommunication between local and central authorities meant it did not obtain the required permits (Liao 2018). Instead, the market has come to be dominated by the domestic massive online platform companies Alibaba, Tencent, and Baidu. Among a list of top 100 mobile apps on the Chinese market as measured in market penetration in 2017, only a handful are produced by a foreign entity (Jiguang n.d.).

In governing online content, Beijing thus has employed a combination of the territorialization (Great Firewall) and indigenization (barring foreign businesses) approaches, with considerable success. This not only has substantial economic benefits, it also provides the leadership with a more effectively governed landscape. Regular tussles notwithstanding, over the years, a modus vivendi has emerged between China's online businesses and the central government. Government recognizes private business has generated considerable economic and technological achievement, and thus maintains a mostly positive attitude, while businesses do not upset the governmental applecart, and are far more trusted on politically sensitive matters than their foreign equivalents (Creemers 2018).

The Domain Name System (DNS)

In the early days of the Internet, China's participation in ICANN was limited, partially due to a comparative lack of Chinese expertise, but also because of

political objections against the structure and politics of ICANN. Some of these objections were quite specific. ICANN, as a private corporation, did not subscribe to usual diplomatic protocols concerning Taiwan. Rather, the Taiwanese government participated equally in ICANN institutions, including the Governmental Advisory Council (GAC). China also found ICANN lagging on technical questions affecting its claims and preferences, particularly in terms of adapting the DNS to adapt Chinese and other non-Roman alphabets. China boycotted ICANN conferences between 2001 and 2009.[2] On these matters, China and ICANN reached an agreement. China would send a MIIT representative to the GAC, while ICANN would refer to Taiwan as "Chinese Taipei." It would also create a fast track for the inauguration of top-level domains (TLDs) in non-Western scripts. Moreover, management powers for the Chinese character TLDs were handed over to CNNIC, providing a further economic incentive for the continued support of the ICANN system (Mueller 2012).

Broader problems in China's perception of ICANN were, perhaps ironically, its multistakeholder functioning on the one hand, and its close relationship with the US government on the other. From 1998 onwards, ICANN had managed the DNS through a contract with the Department of Commerce National Telecommunications and Information Administration, yet governments played a minimal role in its internal processes. On the one hand, China was concerned this meant decisions with potential strategic relevance could be taken outside of governmental control. On the other, there were fears concerning American preponderance in Internet infrastructure and traffic control. A 2012 *People's Daily* piece, for instance, laments (incorrectly) that all thirteen root servers are set up within the United States, and that 80 percent of global Internet traffic passed through the United States (*People's Daily* 2012). These objections pushed China to propose a different arrangement to govern the DNS: ICANN, or its functions, should be brought under the control of the United Nations, or more specifically, under the aegis of the International Telecommunications Union. First presented at the first World Summit on the Information Society (Segal 2017), this position quickly became a core element of its international cyber strategy. Moreover, China was not the only country dissatisfied with the ICANN status quo: India equally proposed transferring responsibilities for Internet governance to the ITU (Shen 2016, 89).

Even so, relationships between Beijing and ICANN have improved considerably over the years. For its part, ICANN has worked hard to establish good relationships with Chinese authorities during this process. It opened its first Engagement Centre in Beijing at the ICANN46 meeting (ICANN 2013). This center liaises closely with authorities in order to build mutual trust and deepen collaboration. Then-ICANN CEO Fadi Chehadé joined the high-level advisory committee for the Wuzhen World Internet Conference as

cochairman (Xinhua 2015). China, equally, has made efforts to build closer relations. The ICANN50 meeting in London, most notably, was the venue for CAC director Lu Wei to make his first high-profile international appearance (Lu 2014). Furthermore, the ICANN transition away from a direct contractual relationship with the US government and toward nongovernmental, multistakeholder stewardship assuaged some of Beijing's concerns vis-à-vis the organization. Even so, some ambivalence remains in China's stance. While ICANN reform seems less of a priority for Beijing, the International Strategy for Cooperation in Cyberspace, as well as the Chinese submission to the UN Open-Ended Working Group on Information and Telecommunications still contain references to the need to create a multilateral Internet governance system, and to ensure that institutions governing strategic Internet resources, such as root servers, remain "truly independent of any state's control" (MFA 2019). Partly, this reflects continuing concerns that, as a U.S.-registered corporation, ICANN could be compelled to limit its services to China, for instance, through a process akin to the Department of Commerce Entity List, which limits, among others, technology exports to specific businesses or institutions. Another element is that numerous other strategic resources, such as the root servers on which the DNS depends, remain owned or operated by US entities, further increasing perceived risk.

In the meantime, China has sought to mitigate some of the risks it saw emanating from the ICANN structure through domestic regulation. Almost from the start, the administration of domain names became a government affair, eschewing the multistakeholder approach adopted elsewhere. In 1997, the newly established CNNIC, under the Chinese Academy of Sciences, became responsible for managing Chinese aspects of the DNS, including administration of the .cn domain (Xue 2004). CNNIC also required notification from server operators using other top-level domains (Ermert and Hughes 2003, 202). 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 preexisting 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 secretively 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

subsidize 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 toward localization. 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 localized 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 (Global Times 2016). 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 2019c). The topography of China's Internet, with only a limited number of international gateways, may facilitate the implementation of this requirement.

Data Protection

Like many governments, the Chinese leadership has identified data as a crucial resource for development, but also a potential source of vulnerability. Many of those risks, such as data leaks leading to fraud and abuse, are domestic, but authorities have also voiced concern over the potential harm stemming from data on Chinese citizens and important businesses flowing abroad. Over the past few years, the leadership has thus sought to centralize its previously fragmented regulatory approach to data protection, and data localization is an important element in new regulations. Localization requirements were already issued for financial and healthcare data in 2011 and 2014 respectively (PBoC 2011; NHFPC 2014). A 2013 technical standard required consent of data subjects for data export (Chander and Le 2014). The cybersecurity law would set a general standard across all sectors. Yet, the exact categorization 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 has been on display in the drafting process of the cybersecurity law. The first draft, from July 2015, determined that "critical information infrastructure operators" must store both citizens' personal information and "other important data" gathered during their operations within Chinese territory. Critical information infrastructure was broadly defined, as "basic information networks providing services such as public correspondence and radio and television broadcasting; important information systems for important industries such as energy, transportation, water conservation, and finance, and public service areas such as electricity, water and gas utilities, medical and sanitation service and social security; military networks and government affairs networks for state organs at the sub districted city level and above; and networks and systems owned or managed by network service providers with massive numbers of users" (NPC 2015). The term "important data" remained undefined. In the second draft, published a year later, it was changed into "important business data" (NPC 2016), following suggestions from domestic stakeholders (NPC 2016A). Even so, this new term equally remained undefined. In response, forty foreign business groups submitted a statement asking for change, yet without success (Bloomberg 2016). The third draft, from November 2016, omitted the word "citizen," suggesting all personal data collected in China, also from non-Chinese nationals, should be stored locally (NPC 2016B, Art. 37). The final, enacted version of the law maintained this provision, and reverted to the original formulation of "important data," still without definition. It also refined the definition of critical information infrastructure, to "public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest" (NPC 2016C).

In April 2017, the first set of draft regulations addressed the export of both personal information and important data, setting out conditions under which this export was to be prohibited and outlining security review requirements for permitted cases (CAC 2017b). These draft regulations also widened the scope of regulated subjects: every "network operator," defined as "the owner of a network, a manager, and a network service provider," would be required to store personal and important data locally. Important data was defined for the first time, albeit vaguely, as "data that is closely related to national security, economic development, and social and public interests, with specific reference to national relevant standards and important data identification

guidelines." A separate technical standard on data export refined the definition, providing a detailed list of specific data and their identifying features in twenty-eight industry sectors (TC260 n.d.). Nonetheless, this list is non-exhaustive, and government departments still retain wide discretion to designate other data as important. In the end, the 2017 draft regulations were not adopted, both due to continuing internal debate and opposition in the WTO under the leadership of the United States and Japan (Lu et al. 2018). Similarly, the technical standard still awaits adoption.

Regulatory efforts regained momentum in the spring of 2019, as two draft regulations emerged: one on general data protection matters, and one on cross-border personal data flows. The former again contained a vaguely worded provision on the export of important data, referring the matter to either the relevant controlling authority or cybersecurity departments. Combining elements from the previous draft regulations and draft standard, it defined important data as "data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety, such as undisclosed government information or large-scale data on the population, genetic health, geography, mineral resources, etc. Important data generally does not include enterprises' production, operations, and internal management information, personal information, etc. (CAC 2019c)." For the export of personal data, it referred to the second, separate draft document. These personal data export regulations, strongly influenced by Europe's GDPR, required all network operators to conduct security assessments before exporting personal data, and to file such operations with provincial cybersecurity authorities. Moreover, they sharply curtailed data gathering activities by foreign entities, stipulating that "overseas organizations, in conducting business activities and when collecting the personal information of domestic users through the Internet and other means, shall fulfill the responsibilities and obligations of network operators in these measures through domestic legal representatives or organizations" (CAC 2019b, Art. 20). At the time of writing, these draft measures have not been approved or taken effect.

The tortuous trajectory of data localization over the past years illustrates the difficult balance regulators seek to strike. There are, on the one hand, clear political and economic incentives to localize 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 when 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.

Tilting the Playing Field

As indicated above, the Chinese government has sought to raise the domestic capabilities of its digital sector through various means, including industrial policy and investment. It has, over the years, published highly detailed plans for the country's informatization (State Council 2016), developed special funding vehicles and structures for information technology, and provided the physical infrastructure it believes necessary. These efforts combine the imperative of economic development with a political goal: domestic players are seen as more secure and amenable to government control than foreign businesses. With this support, and by deftly leveraging the enormous size of the domestic market, Chinese technology businesses have become increasingly competitive with foreign counterparts in numerous sectors. This, in combination with the growing priority of cybersecurity, has raised expectations and intentions that indigenous technology might progressively replace foreign hardware and software.

In some cases, regulations have mandated domestic content for quite some time. For instance, in the area of encryption, China has banned foreign technology since 1999 (Segal 2016, State Council 1999). In 2007, the Ministry of Public Security introduced the first iteration of the multilevel protection system (MLPS) for cybersecurity. This categorizes information networks in five tiers, depending on the potential harm to public and private interests, as well as national security, in case of disruption. Level three and higher networks were required to use domestic cybersecurity technology, and retain domestic cybersecurity monitoring contractors (MPS 2007, Arts. 21, 11). Banking regulators issued standards on "secure and controllable" technology that, in many cases, required technology to be acquired from vendors with at least a presence in China, have domestic intellectual property rights or use domestic encryption tools (Freshfields 2016). However, these regulations were withdrawn following public protests by US officials, as well as quiet lobbying by Chinese banks harboring concerns about being pushed to adopt inferior or less secure technology.

A similar to-and-fro was seen in China's push to indigenize technical standards. In 2003, the Chinese government mandated that all wireless devices sold in China must run WAPI, a domestically developed encryption standard. International standardization bodies such as IEEE and ISO all rejected the standard, Intel announced it would stop shipments of Centrino chip technology, while the US government threatened a WTO suit. It did not take long for China to shelve WAPI at an international level. Even so, foreign device manufacturers ended up providing support for WAPI domestically, indicating the extent to which businesses might comply with Chinese policy, or form local partnerships, even if not legally mandated to do so (Ahmed and Weber

2018). Efforts to popularize a homegrown 3G standard, TD-SCDMA, floundered as the technology was inferior and was only adopted by a few handset makers. This saddled China Mobile, which had been pressured to use the standard against its business judgment, with a severe market disadvantage (Knowledge@Wharton 2011). Another domestic encryption standard, ZUC, fared slightly better: it was approved by the European Telecommunications Standards Institute, and adopted as a voluntary standard by the 3G Partnership Project. In late 2011, the adoption of domestic encryption algorithms became obligatory in 4G networks, which *de facto* mandated ZUC use (MacGregor 2012, 40). However, in 2013, China agreed in negotiations with the United States that ZUC compliance would not be a precondition for market access (USTR 2014).

The MLPS was incorporated in the cybersecurity law, which also created an overlapping mandate to the CAC for critical information infrastructure protection. When new draft regulations for the MLPS were published in June 2018, nearly all references to domestic technology and operators had been removed, with the exception of encryption technology. Instead, the document only explicitly required that operation and maintenance of high-level networks is carried out within Chinese territory (MPS 2018, Art. 29), a requirement that was also present in concurrent draft regulations on critical infrastructure protection (CAC 2017a). The MLPS regulations also banned the unauthorized participation of personnel occupying "critical positions" in highly ranked networks, or those providing cybersecurity services to them, in foreign "cyber attack and defence events," or in other words, hacking competitions (MPS 2018, Art. 54). At the same time, the MLPS draft expanded the scope of level three networks to not only include networks whose disruption affects social stability and national security, but also "particularly gravely" affects the lawful rights and interests of private actors (MPS 2018, Art. 15). The changes in the MLPS do not necessarily constitute a relaxation of constraints on foreign technology. First, the second iteration of the MLPS shifts from a greater focus on self-reporting toward more government audits and scrutiny. Second, a number of supplementary technical standards also affect MLPS, and impose more onerous requirements on operators, including source code delivery and access control (Sacks and Li 2018, 9–10).

Technical standards for cybersecurity are likely to erect market access barriers more broadly. Over the past years, Technical Committee 260 (TC260), which is in charge of developing cybersecurity standards, has published over 300 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 various requirements of

this thicket of standards create a range of possible compliance considerations for foreign entities. Where they mandate source code disclosure, businesses rightly worry about disclosure, leaks, and intellectual property loss. Where they mandate data sharing with Chinese government authorities, they may break laws elsewhere or contribute to reputational damage. They may require developing China-only versions of software and hardware, increasing business costs. Ironically, however, this latter element may also limit the export potential of Chinese enterprises. Moreover, the vagueness of these standards (and, more broadly, the cybersecurity law and its attendant regulations) opens the door for uneven enforcement, either for direct political reasons such as the trade war, or as fallout of interdepartmental bickering. These points are, by the very nature of the system's opacity, necessarily opaque. What is certain is that 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 TC260 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).

Chinese measures increasingly clearly show the imprint of Sino-American strife, and the US actions against Huawei and ZTE. One example of this is the debate that took place in the framework of the security review process for critical network products and specialized cybersecurity products, also introduced in the cybersecurity law. Draft measures from 2019, which 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, security, 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 elements in cybersecurity reviews (CAC 2019a). Moreover, the Chinese government announced it might create an "unreliable entity list," sanctioning foreign businesses boycotting or cutting off supplies to Chinese companies for noncommercial purposes. The Ministry of Foreign Affairs explicitly connected the actual introduction of this list with the extent to which Sino-American trade ties improved (Reuters 2019).

Yet, even if there is broad agreement among Chinese policy makers how foreign technology should be managed, the specific way to do so remains disputed. The controversy surrounding the adoption of a specific version of Windows for government systems provides an instructive example. In the summer of 2017, Ni Guangnan, member of the Chinese Academy of Engineering and a prominent advocate for the development of indigenous

operating systems (Ni 2017B) claimed this version should remain outside the government procurement catalogue (Ni 2017), and more broadly, that government operating systems should be "indigenous and controllable (Ni 2017A)." In response, Wang Jun, general engineer at one of the approved third party security evaluators, the China Information Technology Security Evaluation Centres (CNITSEC), stated that the cybersecurity review regime does not discriminate on the basis of nationality. Moreover, Wang indicated that replacing Windows with an indigenous alternative would "not necessarily [be] the best choice" (Transpacifica 2017), citing switchover costs, software incompatibilities, and software quality as reasons. In contrast, Wang hailed the fact that the government edition was developed by a Sino-US joint venture, in which Microsoft cooperated with the China Electronics Technology Group (CETC), with the aim of providing software better responding to user needs and security requirements. Lastly, Wang argued 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 nonideological or political. Some businesses, such as CETC, care 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 (Shih 2015). The existing installed base of foreign technology and integration with other systems means "rip-and-replace" might be very costly.

It is often claimed that the Chinese government uses its close ties to businesses to advance the cause of national champions. This is especially salient 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 (Li 2019), and specific policy plans often indicate local content targets in various sectors and network systems. Furthermore, state-run media outlets regularly target foreign businesses in order to pressure them toward greater compliance, or send political signals. The technology sector is no exception. In July 2019, for instance, Apple was targeted on national radio for allegedly allowing fake reviews to appear on its App Store (CNR 2019). This compounded an already negative picture for Apple in China: Apple's smartphone share plummeted from a high of 27 percent in 2015 to 5 percent in late 2019 (Kirton 2019). Huawei not only took 42 percent 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 (Rapoza 2019). Moreover, the handset market may provide one example of how American trade sanctions might backfire: Huawei has prepared by developing or sourcing alternatives for technologies it might not be able to access reliably in the future. The Google Android operating system is one of these. 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 (Hall 2019). Given Huawei's global market share, this would be a severe blow to the existing duopoly of Google and Apple technology. Even so, it must be remembered that it is not a complete one-way street, and openness continues in other areas: British Telecom became the first foreign mobile operator to gain a nationwide Chinese operating licence in early 2019 (*China Daily* 2019). Moreover, the difficulties 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 (Triolo 2019). The most important question remains how the decoupling that both the Chinese and American stances are likely to cause will impact the highly integrated global digital economy. With some observers already warning about an "innovation winter" (Houser, forthcoming), sovereignty might come at a high cost.

CONCLUSION AND IMPLICATIONS

China's conception of cyber sovereignty is primarily defensive and reactive, as it aims to ensure CCP control over processes that, in its view, may endanger its leading position. It reflects a legal position, entrenching the party-state's exclusive ability to regulate and police the online world, and rejecting any form of foreign interference. But it is not merely a talking point in international diplomatic processes or a propaganda slogan for domestic consumption. It also refers to the capabilities the leadership deems necessary to realize that legal position in actual reality. To this end, it disposes of a set of policy, legal and regulatory tools that fall under the categories of territorialization, indigenization, and investment.

Within the Chinese policy and academic landscape, cyber sovereignty is nearly universally accepted as a foundation for engagement with global cyber affairs at a matter of principle, and it thus constitutes an organizing principle in domestic cyber governance. Domestic technology use requirements, data localization, increasing scrutiny of foreign content and VPNs, security standards that privilege domestic players and government procurement and subsidy programs are all marshalled in pursuit of sovereignty. Overall, China

has sought to maintain interoperability with the global Internet, at the same time as striving to ensure dominance of indigenous online businesses, as well as technological autonomy to the greatest possible extent. Moreover, the increasing tensions with the United States have fostered a greater sense of urgency and unity in Beijing. Nevertheless, there are considerable arguments and differing views among different constituencies on important questions of how this principle is best realized in practice. How, and in which fields, to collaborate with foreign players, the extent to which specific foreign technologies should be banned from certain fields or merely regulated, and how to determine the sort of data that should be nationalized are still open questions.

This trend has not taken place in a vacuum. China's insistence on cyber sovereignty has both been a response to and a catalyst of broader evolutions in global cyber governance. In some cases, other governments have recognized the desirability of jurisdictional powers, referring explicitly to the sovereignty principle. EU digital commissioner Günther Oettinger, for instance, mentioned "digital sovereignty" as an objective for European digital policy (Tost 2015). Sovereignty was recognized as applying to states' use of information technologies in the 2013 and 2015 reports of the United Nations Group of Governmental Experts (Schmitt and Vihul 2017), and is recognized in the *Tallinn Manual*, a comprehensive expert analysis of how international law applies to cyber operations (Schmitt 2017). China is not the only country to institute data localization policies; the EU's General Data Protection Regulation equally requires local storage of personal data under certain circumstances. As governments increasingly assert control over the digital sphere, and as national security questions grow increasingly prominent in global cyber debates, it seems China's approach to sovereignty has to be seen as part of a complex spectrum. While Beijing's stance seems clear-cut and diametrically opposed to that of the United States and its "like-minded" allies in diplomatic discourse, the complexity of the domestic policy and regulatory landscape reveals a more nuanced picture.

To a significant degree, the difference in approaches reflects the contrast in security concepts between Beijing and its Western counterparts. China primarily defines cybersecurity through the lens of "information security" (CAC 2016a), and focuses on the potential impact the uncontrolled circulation of information might have on political, economic, and social stability. It is thus no surprise that content control has historically been the most elaborate component of the cybersecurity landscape. American and European governments, conversely, have largely defined cybersecurity in technical terms, focusing on the integrity, stability, and functioning of information systems and the data stored on them. This, in turn, explains the attention these governments have directed toward the security of telecommunication networks, and in some cases, resorted to banning Chinese suppliers from their domestic markets. It is

worth remembering that China, thus far, has not banned specific hardware or software makers from its markets. Equally, China puts a far greater emphasis on economic development its cyber policy, while the United States stresses military, intelligence, and other national security questions relatively more. It is likely that these views will converge somewhat over the years, as illustrated by greater Western attention to disinformation campaigns and fake news, and China's efforts to establish a cybersecurity review regime. The United States seems more amenable to greater state influence over economic affairs, while China is building up its cyber military and intelligence capabilities. Yet, even that convergence is unlikely to lead to greater cooperation or coordination. It is overshadowed by the growing U.S.–China tensions, in which technology plays a central role. It seems that, increasingly inevitably, arrangements in cyberspace will reflect unadorned great power competition, with interests overshadowing values in importance, and political expediency replaces pragmatic cooperation as a key virtue.

This has important implications on the future development of both the development of the digital economy, and of interstate relations pertaining to cyber affairs. The global digital economy as it exists today, developed since the 1990s in a context where there were few national and international regimes on matters ranging from data flows to supply chains. The current process of increasing regulatory nationalization inaugurates a new paradigm in which multinational companies must operate. One likely scenario is that the world will fragment into separate spheres of cooperation with high degrees of internal harmonization, and significant barriers between them. An example of this is the supply of telecommunications equipment. If China's push for technology indigenization is matched by other major states, or leads to reciprocal measures, the global market for telecommunications devices may equally become segregated along the lines of political alignment. What will be the impact on global connectivity, data and information flows is an important subject for future research. Yet, the tightrope that China needs to walk is a precarious one. In the diplomatic realm, China's strong insistence on sovereignty has contributed to a low level of trust between Beijing and its major international interlocutors. It also has, thus far, overshadowed the question in which areas, how and for which purposes China can cooperate with other states—even those ostensibly more closely aligned—in order to enhance cyber governance, continue to stimulate interoperability and innovation, and tackle shared issues affecting the global online ecosystem. Yet, in the economic realm, greater economic internationalization and technical interoperability is imperative for the flourishing of China's digital industry. Moreover, the global digital economy is, seemingly inextricably, linked with China as a manufacturing base and market. With the nature of cyber issues increasing in complexity, and tensions increasing in intensity, the way Beijing will seek to

preserve this balance, and how its foreign counterparts will respond, will be a prime factor shaping outcomes in the decades to come.

LIST OF ABBREVIATIONS

CAC: Cyberspace Administration of China
CNNIC: China Internet Network Information Centre
CNR: China National Radio
ICANN: Internet Corporation for Assigned Names and Numbers
MFA: Ministry of Foreign Affairs
MII: Ministry of Information Industry
MIIT: Ministry of Industry and Information Technology
MOFCOM: Ministry of Commerce
MPS: Ministry of Public Security
NHFPC: National Health and Family Planning Commission
NPC: National People's Congress
PBoC: People's Bank of China
SARFT: State Administration of Radio, Film and Television
SCIO: State Council Information Office
SIIO: State Internet Information Office
TC260: Technical Committee 260
USTR: United States Trade Representative
UN: United Nations
WIC: World Internet Conference

NOTES

1. This chapter has been written with the generous support of the Dutch Ministry of Foreign Affairs and the NWO (Netherlands Organization for Scientific Research).

2. Members of the technical community and sector institutions such as the Internet Society of China did attend. Given that these organizations function under party leadership and maintain direct connections with the bodies in charge of Internet governance, this meant that Chinese governmental preferences were still represented, albeit indirectly.

BIBLIOGRAPHY

Ahmed, Shazeda and Steven Weber. 2018. "China's Long Game in Techno-Nationalism." *First Monday* 23 (5–7). http://dx.doi.org/10.5210/fm.v23i5.8085.

Arsène, Séverine. 2012. "The Impact of China on Global Internet Governance in an Era of Privatized Control." Presented at the *Chinese Internet Research Conference*, Los Angeles, May 2012. Accessed November 25, 2019. http://hal.archives-ouvertes.fr/hal-00704196/document.

Bloomberg. 2016. "China Adopts Cybersecurity Law Despite Foreign Opposition." November 7, 2016. Accessed November 29, 2019. https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition.

CAC. 2016a. "Guojia wangluo kongjian anquan zhanlüe (National Cyberspace Security Strategy)." December 27, 2016. Translation, accessed November 22, 2019. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/

CAC. 2016b. "Wangluo chuban fuwu guanli guiding (Online Publishing Service Management Rules)." February 4, 2016. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2016/02/04/online-publishing-service-management-rules/

CAC. 2017a. "Guanjian xinxi jichu sheshi anquan baohu tiaoli (zhengqiu yijian gao) (Critical Information Infrastructure Security Protection Regulations)." July 10, 2017. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/

CAC. 2017b. "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))." April 11, 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. 2019a. "Wangluo anquan shencha banfa (zhenqiu yijian gao) (Cybersecurity Review Measures (Draft for Comment))." May 21, 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/

CAC. 2019b. "Shuju anquan guanli banfa (zhenqiu yijian gao) (Data Security Management Measures (Draft for Comment)." May 28, 2019. Translation, accessed November 29, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/

CAC. 2019c. "Geren xinxi chujing anquan pinggu banfa (zhengqiu yijian gao) (Personal Information Outbound Transfer Security Assessment Measures (Draft for Comment)." June 13, 2019. Translation, accessed November 29, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/

Central Committee and State Council. 2016. "Guojiaxinxihua fazhan zhanlüe gangyao (Outline of the National Informatization Development Strategy)." July 27, 2016. Translation, accessed November 22, 2019. https://chinacopyrightandmedia

.wordpress.com/2016/07/27/outline-of-the-national-informatization-development-strategy/

Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." *UC Davis Legal Studies Research Paper Series* 378. Accessed November 29, 2019. https://aicasia.org/wp-content/uploads/2017/06/SSRN-id2407858-1.pdf.

Chang, Gordon G. *The Coming Collapse of China*. New York: Random House, 2010.

China Daily. 2019. "BT Becomes First Foreign Telecoms Firm to Secure Chinese License." January 29, 2019. Accessed November 29, 2019. http://www.chinadaily.com.cn/a/201901/29/WS5c4fbdfca3106c65c34e70b2.html.

CNNIC. 2019. "Di 44 ci 'Zhongguo hulian wangluo fazhan zhuankuang tongji baogao' (44th 'China Statistical Report on Internet Development')." August 30, 2019. Accessed October 19, 2019. http://www.cac.gov.cn/2019-08/30/c_1124938750.htm.

CNR. 2019. "App Store xian 'shuahaoping' wudao yonghu kewu: ruo bu manyi ke gei chaping ('Good Review Paint" Emerges on App Store, Misleading Customers: In Case of Dissatisfaction, Bad Marks May be Awarded)." July 8, 2019. Accessed November 29, 2019. http://china.cnr.cn/yaowen/20190708/t20190708_524682741.shtml.

Congressional Research Service. 2018. "Tricks of the Trade: Section 301 Investigation of Chinese Intellectual Property Practices Concludes." March 29, 2018. Accessed November 29, 2019. https://crsreports.congress.gov/product/pdf/LSB/LSB10109.

Corera, Gordon. 2015. *Intercept: The Secret History of Computers and Spies*. London: Hachette UK.

Creemers, Rogier. 2018. "Disrupting the Chinese State: New Actors and New Factors." *Asiascape: Digital Asia* 5(3): 169–197.

Creemers, Rogier. 2019. "The International and Foreign Policy Impact of China's Artificial Intelligence and Big-Data Strategies." In *Artificial Intelligence, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives*, edited by Wright, Nicholas, 129–135. Maxwell AFB: Air University Press.

Demchak, Chris. 2016. "Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age." *The Cyber Defense Review* 1(1): 49–74.

Dutton, William H., and Malcolm Peltu. 2008. "The New Politics of the Internet: Multi-stakeholder Policy-making and the Internet Technocracy." In: *Routledge handbook of Internet politics*, edited by Chadwick, Andrew and Philip Howard, 400–416. Abingdon: Routledge.

Ermert, Monika and Christopher Hughes. 2003. "What's in a Name? China and the Domain Name System." In: *China and the Internet: Politics of the Digital Leap Forward*, edited by Hughes, Christopher and Gudrun Wacker, 127–138. Abingdon: Routledge.

Feng, Emily. 2018. "China's State-Owned Venture Capital Funds Battle to Make an Impact." *Financial Times.* December 23, 2018. Accessed November 29, 2019. https://www.ft.com/content/4fa2caaa-f9f0-11e8-af46-2022a0b02a6c.

Forster, Elisabeth. 2018. *1919—The Year That Changed China: A New History of the New Culture Movement*. Berlin: De Gruyter.

Freshfields. 2016. "China Introduces Comprehensive New Cyber Security Rules for Banking Procurement." Accessed November 29, 2019. http://knowledge.freshfields.com/m/Global/r/1514/china_introduces_comprehensive_new_cyber_security_rules.

Glanville, Luke. 2013. *Sovereignty and the Responsibility to Protect: A New History*. Chicago: University of Chicago Press.

Global Times. 2016. "Hulianwang xingui bing fei 'fengsha jingwai wangzhan', IT jie wangyou jiedu zhuanye shuyu (New Internet Rules Don't 'Wipe Out Foreign Websites', Netizens from IT Circles Explain Specialized Jargon)." March 29, 2016. Accessed November 29, 2019. https://world.huanqiu.com/article/9CaKrnJUT0p.

Griffiths, James. *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. London: Zed Books.

Hall, Chris. 2019. "Huawei HarmonyOS Update: Without Google What Is Huawei's plan B?" *Pocket Lint.* September 18, 2019. Accessed November 29, 2019. https://www.pocket-lint.com/phones/news/huawei/148118-huawei-alternative-os-without-google-huawei-plan-b.

Harold, Scott Warren, Martin C. Libicki, and Astrid Stuth Cevallos. 2016. "Getting to Yes with China in Cyberspace." *Rand Corporation*. Accessed November 25, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

Houser, Kimberley. Forthcoming. "The Innovation Winter Is Coming: How the U.S.-China Trade War Endangers the World." *San Diego Law Review* 57(3). Accessed November 29, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473902.

https://opinion.huanqiu.com/article/9CaKrnK3qF3.

Hu, Jintao. 2011. "Jianding buyi zou Zhongguo tese shehuizhuyi wenhua fazhan daolu: nuli jianshe shehuizhuyi wenhua qiangguo (Resolutely Walk the Path of Socialist Culture Development with Chinese Characteristics: Striving to Construct a Strong Socialist Culture Country)." *Qiushi*. Translation, accessed November 28, 2019. https://chinacopyrightandmedia.wordpress.com/2012/01/04/hu-jintaos-article-in-qiushi-magazine-translated/

ICANN. 2013. "ICANN Engagement Center to Open In Beijing." April 8, 2013. Accessed November 29, 2019. https://www.icann.org/en/system/files/press-materials/release-08apr13-en.pdf.

Jiguang. S.d. "Jiguang dashuju: 2017 nian yidong hulianwang hangye pandian app bangdan (Jiguang data: a 2017 list of apps in the mobile Internet sector)." Accessed November 29, 2019. https://www.jiguang.cn/reports/195.

Kai, Jin. 2014. "Why China Banned Windows 8." *The Diplomat.* May 28, 2014. Accessed November 29, 2019. https://thediplomat.com/2014/05/why-china-banned-windows-8/.

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.

Kirton, David. 2019. "Huawei Tightens China Market Hold with 42% Share at Expense of iPhones: Canalys." *Reuters.* October 30, 2019. https://www.reuters.

com/article/us-china-smartphone/huawei-tightens-china-market-hold-with-42-share-at-expense-of-iphones-canalys-idUSKBN1X907R.
Klimburg, Alexander. 2013. "The Internet Yalta." *Center for a New American Security*. Accessed November 29, 2019. http://dragon-report.com/Dragon_Report/home/home_files/The%20Internet%20Yalta.pdf.
Knowledge@Wharton. 2011. "China's 3G Technology Gamble: Who Has the Last Laugh?" Accessed November 29, 2019. https://knowledge.wharton.upenn.edu/article/chinas-3g-technology-gamble-who-has-the-last-laugh/
Kolton, Michael. 2017. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2(1), 119–154.
Krasner, Stephen D. 1999. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press.
Lee, Jyh-An. 2018. "Great Firewall." *The Chinese University of Hong Kong Faculty of Law Research Papers* 2018–10.
Li, Tao. 2019. "Huawei Wins Half of China Mobile's 5G Network Contracts While Ericsson Picks Up a Third." *South China Morning Post.* June 17, 2019. https://www.scmp.com/tech/big-tech/article/3014766/china-mobile-awards-half-its-5g-network-contracts-huawei-while.
Liao, Shannon. 2018. After a Single Day, Facebook Is Pushed Out of China Again." *The Verge.* July 25, 2018. Accessed November 29, 2019. https://www.theverge.com/2018/7/25/17612162/facebook-technology-subsidiary-blocked-china-censor.
Lindsay, Jon. 2014. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39(3): 7–47.
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)." October 30, 2013. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2013/10/30/siio-director-outlines-eight-objectives-for-online-media/.
Lu, Wei. 2014. "Gongxiang de wangluo, gongzhi de kongjian: zai ICANN Lundun huiyi kaimushi de zhuzhi yanjiang (A Network Shared Together, A Space Governed Together: Keynote Speech at the Opening Ceremony of the London ICANN Meeting)." June 23, 2014. Translation, accessed November 22, 2019. https://chinacopyrightandmedia.wordpress.com/2014/06/23/a-network-shared-together-a-space-governed-together/
Lu, Xiaomeng, Paul Triolo, Samm Sacks, Rogier Creemers, and Graham Webster. 2018. "Progress, Pauses, and Power Shifts in China's Cybersecurity Law Regime." *Digichina*. Accessed November 29, 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/progress-pauses-power-shifts-chinas-cybersecurity-law-regime/
Macmillan, Margaret. 2011. *Peacemakers: Six Months That Changed the World*. London: Hachette, UK.
Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson. 2015. "China's Great Cannon." *CitizenLab*. Accessed November 29, 2019. https://citizenlab.ca/wp-content/uploads/2009/10/ChinasGreatCannon.pdf.

McGregor, James. 2012. *No Ancient Wisdom, No Followers: The Challenges of Chinese Authoritarian Capitalism*. London: Easton Studio Press.

MFA. 2012. "Statement at Budapest Conference on Cyber Issues." October 4, 2012. Accessed November 22, 2019. http://www.chinesemission-vienna.at/eng/zgbd/t977627.htm.

MFA. 2017. "Wangluo kongjian guoji hezuo zhanlüe (International Strategy of Cooperation on Cyberspace)." January 3, 2017. Translation, accessed November 22, 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 November 29, 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

MII. 2002. "Zhongguo hulianwangluo yuming guanli banfa (Management Rules for Domain Names on the Chinese Internet)." August 1, 2002. Accessed November 29, 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 November 29, 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))." March 25, 2016. Translation, accessed November 29, 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)." August 16, 2017. Accessed November 29, 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.

Mitter, Rana. 2013. *China's War with Japan, 1937–1945: The Struggle for Survival.* London: Penguin.

MOFCOM. 2001. "China's Schedule of Specific Commitments." Accessed November 29, 2019. http://fta.mofcom.gov.cn/pakistan/xieyi/fwmyxieding-zfcrb_en.pdf.

Morrison, Aimée Hope. "An Impossible Future: John Perry Barlow's' Declaration of the Independence of Cyberspace'." *New Media & Society* 11(1-2): 53-71.

MPS. 2007. "Xinxi anquan dengji baohu guanli banfa (Information Security Multi-level Protection Management Rules)." June 22, 2007. Accessed November 29, 2019. http://www.gov.cn/gzdt/2007-07/24/content_694380.htm.

MPS. 2018. "Wangluo anquan dengji baohu tiaoli (zhenqiu yijian gao) (Cybersecurity Multi-level Protection Management Rules (Opinion-seeking Draft)." June 27, 2018. Accessed November 29, 2019. http://www.mps.gov.cn/n2254536/n4904355/c6159136/content.html.

Mueller, Milton. 2012. "China and Global Internet Governance: A Tiger By the Tail." In A*ccess Contested: Security, Identity and Resistance in Asian Cyberspace*, edited by Deibert, Ronald, 177–194. Cambridge: MIT Press.

NHFPC. 2014. "Renkou jiankang xinxi guanli banfa (shixing) (Population Health Information Management Rules (Trial))." May 5, 2014. Accessed November 29, 2019. http://www.cac.gov.cn/2014-08/20/c_1112064075.htm.

Ni, Guangnan, 2017A. "Zhengfu caozuo xitong ying quebao zizhu kekong (Government Operating Systems Should Be Guaranteed Indigenous and Controllable)." *Global Times.* June 13, 2007. Accessed November 29, 2019.

Ni, Guangnan. 2017. "Jianyi zhengfu tingzhi caigou he shiyong 'Win10 zhengfuban' (I Suggest the Government Ceases to Buy and Use the 'Win10 Government Edition')." *QQ Tech.* June 8, 2017. Accessed November 9, 2019.

Ni, Guangnan. 2017B. "Jiandingbuyi de fazhan guochan caozuo xitong (Unwaveringly Develop Domestically Produced Operating Systems)." *Global Times*. June 29, 2017. Accessed November 29, 2019. https://opinion.huanqiu.com/article/9CaKrnK3MJr.

NPC. 2015. "Zhonghua renmin gongheguo wangluo anquan fa (cao'an) (Cybersecurity Law of the People's Republic of China (Draft))." July 6, 2015. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2015/07/06/cybersecurity-law-of-the-peoples-republic-of-china-draft/

NPC. 2016. "Zhonghua renmin gongheguo wangluo anquan fa (cao'an—erci shenyi gao) (Cybersecurity Law of the People's Republic of China (Second Reading Draft)." July 6, 2016. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2016/07/06/peoples-republic-of-china-cybersecurity-law-second-reading-draft/

NPC. 2016. "Zhonghua renmin gongheguo wangluo anquan fa (cao'an—sanci shenyi gao) (Cybersecurity Law of the People's Republic of China (Third Reading Draft)." November 2, 2016. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2016/11/02/cybersecurity-law-of-the-peoples-republic-of-china-third-reading-draft/

NPC. 2016A. "Wangluo anquan fa (cao'an) de xiugai qingkuang (The Situation of the Revision of the Cybersecurity Law (Draft))." July 8, 2016. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2016/07/08/the-situation-of-the-revision-of-the-cybersecurity-law-draft/

NPC. 2016C. "Zhonghua renmin gongheguo wangluo anquan fa (Cybersecurity Law of the People's Republic of China." November 7, 2016. Translation, accessed November 22, 2019. https://chinacopyrightandmedia.wordpress.com/2016/11/07/cybersecurity-law-of-the-peoples-republic-of-china/

Panda, Ankit. 2019. "Huawei's Legal Woes and Tech 'Decoupling' Between China and the West." *The Diplomat*. February 4, 2019. Accessed November 29, 2019. https://thediplomat.com/2019/02/huaweis-legal-woes-and-tech-decoupling-between-china-and-the-west/

PBoC. 2011. "Guanyi yinhangye jinrong jigou zuohao geren jinrong xinxi baohu gongzuo de tongzhi (Notice concerning Protecting Personal Financial Information in Financial Bodies in the Banking Sector)." January 21, 2011. Accessed November 29, 2019. http://www.gov.cn/gongbao/content/2011/content_1918924.htm.

Pei, Minxin. 2006. *China's Trapped Transition*. Cambridge: Harvard University Press.

People's Daily. 2012. "Wangzhan xiaoyenmiman, women ruhe yingdui (Smoke over the Network Warfare Battlefield, How Do We Respond)." June 6, 2012. Accessed November 29, 2019. http://media.people.com.cn/GB/18088684.html.

People's Daily. 2014. "Guojia Hulianwang Bangongshi fuzhuren Wang Xiujin: wangluo anquan shi zhongda zhanlüe wenti (SIIO Vice-Director Wang Xiujun: Cybersecurity Is a Major Strategic Question)." May 18, 2014. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2014/05/30/siio-vice-director-wang-xiujun-cybersecurity-is-a-major-strategic-question/

Qu, Weizhi. 2010. *China's Path to Informatization*. Singapore: Cengage Learning Asia.

Rapoza, Kenneth. 2019. "Huawei Has Taken Over Apple's Market Share in China; It Will Get Worse." *Forbes.* May 2, 2019. Accessed November 29, 2019. https://www.forbes.com/sites/kenrapoza/2019/05/02/huawei-has-taken-over-apples-market-share-in-china-it-will-get-worse/#3530820385f1.

Reuters. 2019. China Publication of 'Unreliable Entities List' Depends on Sino-U.S. Trade Talks: Sources." October 11, 2019. Accessed November 29, 2019. https://www.reuters.com/article/us-usa-trade-china-entities/china-publication-of-unreliable-entities-list-depends-on-sino-u-s-trade-talks-sources-idUSKBN1WQ28L.

Sacks, Samm and Manyi Kathy Li. 2018. "How Chinese Cybersecurity Standards Impact Doing Business in China." *CSIS Briefs*. Accessed November 29, 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf?EqyEvuhZiedaLDFDQ.7pG4W1IGb8bUGF.

SARFT. 2000. "Xinxi wangluo chuanbo guangbo dianying dianshi lei jiemu jiandu guanli zanxing banfa (Provisional Information Network Dissemination of Radio, Film and Television-Type Programme Supervision and Management Rules)." April 7, 2000. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2000/04/07/provisional-information-network-dissemination-of-radio-film-and-television-type-programme-supervision-management-rules/

SARFT. 2004. "Hulianwang deng xinxi wanluo chuanbo shiting jiemu guanli banfa (Internet and Other Information Networks Audiovisual Programme Dissemination Management Rules)." July 6, 2004. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2004/07/06/internet-and-other-information-networks-audiovisual-programme-dissemination-management-rules/

Schell, Orville, and John Delury. 2014. *Wealth and Power: China's Long March to the Twenty-First Century*. New York: Random House, 2014.

Schmitt, Michael N., and Liis Vihul. 2017. "Sovereignty in Cyberspace: Lex Lata Vel Non?" *AJIL Unbound* 111: 213–218.

Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

SCIO and MII. 2005. "Hulianwang xinwen xinxi fuwu guanli guiding (Internet News Information Service Management Regulations)." September 25, 2005. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2005/09/25/internet-news-information-service-management-regulations/

SCIO. 2010. "The Internet in China (White Paper)." June 8, 2010. Accessed October 22, 2019. http://www.chinadaily.com.cn/china/2010-06/08/content_9950198.htm.

SCMP. 2018. "Timeline: Chinese Telecoms Giants Huawei, ZTE Incur Wrath of Washington Over Iran Sanction Violations." December 6, 2018. Accessed November 29, 2019. https://www.scmp.com/tech/big-tech/article/2176664/timeline-chinese-telecoms-giants-huawei-zte-incur-wrath-washington.

Segal, Adam. 2016. "China, Encryption Policy, and International Influence." *Hoover Institution.* Accessed November 29, 2019. https://www.hoover.org/sites/default/files/research/docs/segal_webreadypdf_updatedfinal.pdf.

Segal, Adam. 2017. "Chinese Cyber Diplomacy in a New Era of Uncertainty." *Hoover Institution, Aegis Paper Series* 1703. Accessed November 29, 2019. https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf.

Sevastopulo, Demetri and Geoff Dyer. 2015. "Obama and Xi in Deal on Cyber Espionage." *Financial Times.* September 15, 2015. Accessed November 29, 2019. https://www.ft.com/content/0dbcab36-63be-11e5-a28b-50226830d644.

Shen, Hong. 2016. "China and Global Internet Governance: Toward an Alternative Analytical Framework." *Chinese Journal of Communication* 9(3): 304–324.

Shen, Hong. 2018. "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative." *International Journal of Communication* 12: 2683–2701.

Shen, Yi. 2016. "Cyber Sovereignty and the Governance of Global Cyberspace." *Chinese Political Science Review* 1(1): 81–93.

Shih, Gerry. 2015. "Huawei CEO Says Chinese Cybersecurity Rules Could Backfire." *Reuters.* April 21, 2015. Accessed November 29, 2019. http://www.reuters.com/article/2015/04/21/us-huawei-cybersecurity-idUSKBN0NC1G920150421.

State Council. 1999. "Shangyong mima guanli guiding (Commercial Encryption Management Regulations)." October 7, 1999. Accessed November 29, 2019. https://zh.wikisource.org/zh-hans/中华人民共和国国务院令第273号

State Council. 2000. "Hulianwang xinxi fuwu guanli banfa (Internet Information Service Management Rules)." September 25, 2000. Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2000/09/25/internet-information-service-management-rules/

State Council. 2016. "'Shisan wu' guojia xinxihua guihua ('13th Five-Year Plan' for National Informatization)." December 15, 2016. Accessed November 29, 2019. http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm.

Stein, Arthur A. 2016. "The Great Trilemma: are Globalization, Democracy, and Sovereignty Compatible?" *International Theory* 8(2): 297-340.

TC260. n.d. "Xinxi anquan jishu—shuju chujing anquan pinggu zhinan (Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment)." Accessed November 29, 2019. https://www.tc260.org.cn/ueditor/jsp/upload/20170527/87491495878030102.pdf.

Thomas, Daniel C. 2001. *The Helsinki Effect: International Norms, Human Rights, and the Demise of Communism*. Princeton: Princeton University Press.

Thomas, Neil. 2019. "Mao Redux: The Enduring Relevance of Self-Reliance in China." *MacroPolo.* April 25, 2019. Accessed November 29, 2019. https://macropolo.org/analysis/china-self-reliance-xi-jin-ping-mao/

Tost. 2015. "Oettinger Calls for 'Europeanisation' of Digital Policy." *EurActiv.* March 17, 2015. Accessed November 29, 2019. https://www.euractiv.com/section/digital/news/oettinger-calls-for-europeanisation-of-digital-policy/

TransPacifica. 2017. "Chinese IT Security Examiner Describes Review Process, Clarifies Status of Chinese Government Windows Edition." Accessed November 29, 2019. http://transpacifica.net/2017/06/1963/

Triolo, Paul. 2019. "China Is Not A Technology Superpower. Stop Treating It Like One." *SupChina.* October 1, 2019. https://supchina.com/2019/10/01/china-is-not-a-technology-superpower-stop-treating-it-like-one/

UN. 2011. "International Code of Conduct for Information Security." A/66/339. September 12, 2011. Accessed October 22, 2019. https://www.un.org/ga/search/view_doc.asp?symbol=A%2F66%2F359&Submit=Search&Lang=E.

UN. 2015. "International Code of Conduct for Information Security." A/69/723. January 9, 2015. Accessed October 22, 2019. https://digitallibrary.un.org/record/786846/files/A_69_723-EN.pdf.

USTR. 2014. "Fact Sheet: Successes in Reducing Technical Barriers to Trade to Open Markets for American Exports." Accessed November 29, 2019. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2014/March/Successes-Reducing-Technical-Barriers-to-Trade-to-Open-Markets-for-US-Exports.

Waddell, Kaveh. 2016. "Why Google Quit China—and Why It's Heading Back." *The Atlantic*. Accessed November 29, 2019. https://www.theatlantic.com/technology/archive/2016/01/why-google-quit-china-and-why-its-heading-back/424482/

Wang Yonggui. 2011. "Zhongguo gongchandang 90 nian lai tuijin yishixingtai gongzuo de lishi jingyan (The Historical Experience of the Chinese Communist Party's 90 Years of Moving Ideological Work Forward)." Translation, accessed October 19, 2019. https://chinacopyrightandmedia.wordpress.com/2011/09/09/the-historical-experience-of-the-chinese-communist-partys-90-years-of-moving-ideological-work-forward/

Wang, Yubian, and Yuri Shebzukhov. 2019. "From Network Security to Network Autonomous." *International Journal of Advanced Network, Monitoring and Controls* 4(1): 61–65.

Wang, Yuhua, and Carl Minzner. 2015. "The Eise of the Chinese Security State." *The China Quarterly* 222: 339–359.

WIC. 2014. "Wuzhen Declaration." November 21, 2014. On file with author.

Wübbeke, Jost, Mirjam Meissner, Max J. Zenglein, Jaqueline Ives and Björn Conrad. 2016. "Made in China 2025." *MERICS Papers on China* 2016(2). Accessed 29 November 2019. https://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf.

Xi, Jinping. 2013. "Zai quanguo xuanchuan sixiang gongzuo huiyi de jianghua (Speech at the Nationwide Propaganda and Ideology Work Conference)." August 19, 2013. Trranslation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2013/11/12/xi-jinpings-19-august-speech-revealed-translation/

Xi, Jinping. 2015. "Zai di'er jie shijie hulianwang dahui kaimushi de jianghua (Speech at the 2nd World Internet Conference Opening Ceremony)." December 16, 2015. Translation, accessed November 22, 2019. https://chinacopyrightandmedia.wordpress.com/2015/12/16/speech-at-the-2nd-world-internet-conference-opening-ceremony/

Xinhua. 2015. "High-level Advisory Committee Established for World Internet Conference." December 21, 2015. Accessed November 29, 2019. http://www.wuzhenwic.org/2015-12/21/c_48303.htm.

Xue, Hong. 2004. "Voice of China: A Story of Chinese-Character Domain Names." *Cardozo Journal of International and Comparative Law* 12: 559–592.

Yuan, Li. 2019. "As Huawei Loses Google, the U.S.-China Tech Cold War Gets Its Iron Curtain." *New York Times*, May 20, 2019. https://www.nytimes.com/2019/05/20/business/huawei-trump-china-trade.html.

Zeng, Jinghan, Tim Stevens and Yaru Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'." *Politics & Policy* 45(3): 432–464.

Zhao, Zhoujian and Zhilian Xu. 2014. "Xinxi jiashu fazhan qushi yu yishixingtai anquan (Information Technology Development Trends and Ideological Security)." *Red Flag Manuscripts.* Translation, accessed November 29, 2019. https://chinacopyrightandmedia.wordpress.com/2015/01/01/information-technology-development-trends-and-ideological-security/.