3

# The Spatial Expansion of China's Digital Sovereignty

## *Extraterritoriality and Geopolitics*

Wanshu Cong

### 3.1 INTRODUCTION

For various historical and political reasons, the idea of digital sovereignty, and the concept of sovereignty more broadly, is largely a state-centric one in China, revolving around the discourse, policies, and practices of the Chinese government. Within the history of the internet, China has a relatively long tradition of proclaiming cyber sovereignty and establishing state control over the cyberspace and digital infrastructures. Various practices of China bordering or "re-territorializing" the cyberspace (Kettemann, 2020) demonstrate this sovereigntist approach of governing the internet, such as the Great Firewall that censors the transmission of information to China, and the rule of data localization prescribed by Article 37 of China's *Cyber Security Law* (CSL). Deep political and ideological reasons make it unlikely for China to depart from its adherence to the sovereigntist approach for governing the internet. However, the application of strict territoriality principle to the governance of the internet has indeed been challenged by its high economic costs and lack of efficacy to protect the expanding market and interest of Chinese tech and digital companies overseas. These challenges called for new ways of understanding the scope and substance of state digital sovereignty and of exercising its sovereign power over the internet and data. The Chinese regulatory evolution appears to be a gradual spatial expansion of its regulatory power beyond the physical borders, reflecting an emerging tendency from territoriality to extraterritoriality in the conception and practice of China's digital sovereignty. This tendency is what this chapter inquires.

Of course, one may ask whether there is really a shift from territoriality to extraterritoriality in the cyber context.[1] In addition, despite its attempts of grafting borders onto the internet, China is no less reluctant to undertake

[1] Notes: See discussions about the extraterritorial effect of territorial control of the internet, for example (Hildebrandt, 2013; Mueller, 2010).



https://doi.org/10.1017/9781009531085.005 Published online by Cambridge University Press

extraterritorial measures against dissidents, and, therefore, its seemingly territorial approach does not reflect the complexity of actual practices. The chapter does not present this tendency as a sudden new phenomenon. What is interesting, however, is that the mismatch between China's official stance and actual practice may become less stark due to the emerging change of regulatory philosophy: the regulatory tendency toward extraterritoriality can be identified explicitly in recent initiatives as well as scholarly discussions. They differ from previous practices of which extraterritoriality is rather implicit and barely gets clear legal justifications.

This chapter, adopting a state-centric perspective of digital sovereignty (see Chapter 1), draws attention to China's three recent regulatory instruments, which most remarkably demonstrate the direction toward the spatial expansion of China's digital sovereignty: China's Personal Information Protection Law ("the PIPL"),[2] Data Security Law ("the DSL"),[3] and the order by the Ministry of Commerce on blocking unjustified extraterritorial application of foreign legislation and measures ("the Blocking Rules"). In Section 3.2, I discuss two approaches of broadening the spatial dimension of China's state digital sovereignty, which can be identified in these three instruments. The first one is to include extraterritorial rules in data governance legislation, making such legislation applicable beyond China's territory or produce extraterritorial impacts. The other approach is to resort to blocking or countering measures against certain foreign measures related to data that China deem illegitimate. While their practical effects need more time to manifest, they demonstrate a clear intention of the Chinese government to regulate extraterritorially data, data activities (such as data collection, processing, and transfer) and data-related activities (such as trade and investment in relation to data), and hence to expand the spatial scope of China's digital sovereignty. International environment is indispensable to understanding this regulatory and conceptual evolution. Accordingly, given the current, increasingly confrontational international context, I argue in Section 3.3 that this regulatory evolution represents a greater incorporation of geostrategic interests in China's conception and practice of digital sovereignty, as a response to the geopolitical challenges that China is facing.

While the term "digital sovereignty" may be intuitively related to having and exercising control over data and digital infrastructures (Floridi, 2020), it remains highly controversial and has varied meanings for different societies (see Chapter 1).[4] For this chapter, as it analyzes and interprets recent

[2] The law was passed on August 20, 2021 and entered into force on November 1, 2021.

[3] The law was passed on June 10, 2021 and entered into force on September 1, 2021.

[4] Highly contestable issues include, for example, who is endowed with digital sovereignty, how does different actors' control relate to each other, whether "digital sovereignty" necessarily lead to trade protectionism and restrictions of individual rights and whether "digital sovereignty" can empower countries to resist the domination of foreign tech giants and lead to a more just redistribution of power and resources.

legislative and policy initiatives, it pays less attention to theorizing what "digital sovereignty" means. Instead, I use "digital sovereignty" as a composite term to refer to state authority over digital technologies and their social, political, and economic impacts. To justify this broad use of the term within the state-centric perspective, it suffices to say that in the Chinese context, as data is deemed as "fundamental strategic resources" since the thirteenth five-year plan (NPC & Central Committee of the CPC, 2016) and an important factor of production (Huang et al., 2020; Shi, 2018), digital sovereignty is as much about infrastructural and technological sovereignty as about economic sovereignty and hence is inherently multidimensional. As will be seen, this imbrication of the digital with the material is reflected by the way how the notion of digital sovereignty incorporates both geostrategic interests of the state and private economic interests. Given changes in these two interests in the current international environment, the spatial expansion of China's digital sovereignty should not be surprising.

## 3.2 TWO APPROACHES TOWARD EXTRATERRITORIALITY

Two approaches toward the spatial expansion of China's digital sovereignty can be identified in the three instruments. The first and the most straightforward approach is to explicitly adopt extraterritorial rules in the PIPL and the DSL. The second approach, present in all three instruments, is to block or counter certain foreign measures deemed discriminatory or restrictive against China.

### 3.2.1 Extraterritoriality in Data Governance Legislation

The attempts of re-territorializing the cyberspace and data flows by the CSL, reflecting a more exclusive and territorialized conception of cyber sovereignty and greater securitization of the internet, have been criticized widely both inside and outside of China. In terms of the territorial scope of application, the CSL applies only to the construction, operation, maintenance and use of network, and cybersecurity supervision and management within the territory of the People's Republic of China.[5] Regarding cross-border data transfer, the default rule in the CSL is for critical information infrastructure operators to store personal information and important data that they collect within China.[6] The PIPL and DSL differ considerably from the CSL in both aspects. With respect to extraterritorial application, the PIPL applies to the following situations where activities of handling personal information of natural persons in China take place outside of China:

[5] CSL, Article 2.
[6] CSL, Article 37.

1. When the purpose of such activity is to provide products or services to natural persons within China,
2. When analyzing or assessing activities of natural persons within China, and
3. Other circumstances provided by laws or administrative regulations.

To give teeth to the extraterritorial scope of this law, Article 42 of the PIPL addresses enforcement issues. It authorizes the Chinese cybersecurity and informatization department to impose administrative sanctions on foreign organizations or individuals whose personal information handling activities create harms on the rights and interests of Chinese citizens or on China's national security or public interest.[7]

As for the DSL, apart from data activities carried out within China, Article 2(2) sets out that "data processing activities outside China which harm China's national security, public interest or lawful rights and interests of citizens and organizations, are to be pursued for legal responsibility in accordance with the law." These provisions of extraterritorial application in these two instruments illustrate an exercise of legislative jurisdiction that combines the principle of territoriality and the effects doctrine, making the location of the effect of data activities a crucial factor for re-territorializing the cyberspace.

With respect to cross-border data flows, Article 38 of the PIPL sets out four options for transferring personal information abroad, easing the data localization rule in CSL:[8]

1. passing a security assessment organized by the State cybersecurity and informatization department,
2. obtaining personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department,
3. concluding an agreement with a foreign receiving party according to the standard contract formulated by the State cybersecurity and informatization departments, which sets out the rights and obligations of the parties,
4. other conditions provided by the State cybersecurity and informatization department in laws or administrative regulations.

In addition to these options, personal information handlers are required to ensure that the treatment of personal information transferred abroad is up to the standard of this law.[9] Furthermore, these options are followed by

[7] The sanctions include putting such organizations or individuals on a list that would limit or prohibit the provision of personal information to them, issuing a warning, or limiting or prohibiting the provision of personal information to them.

[8] These conditions do not apply to international agreements or treaties that China joins which contains requirements for sending personal information outside China. See, PIPL, Article 38, para 2.

[9] PIPL, Article 38, para 3.

the obligations of individual notification, obtaining individual consent,[10] and conducting risk assessments by those who seek to export personal information.[11] A default data localization requirement still exists in the PIPL and applies to critical information infrastructure operators and those entities who process personal information up to certain quantities determined by the State cybersecurity and informatization department. For these two categories of data collecting/processing entities, only the first option in Article 38 is available.[12]

The DSL introduces a single article addressing the export of data upon requests by foreign governmental authorities.[13] According to this provision, such requests shall be dealt with in accordance with relevant laws and international agreements and conventions to which China is a party, or according to the principle of equality and reciprocity; without the approval of relevant competent departments of China, no data stored within China shall be transferred abroad upon such requests. Organizations or individuals within China that violate this provision will face administrative sanctions.[14] A similar provision also exists in the PIPL.[15] Beyond this particular scenario, the DSL does not say much about cross-border data transfers. Article 31 specifies that the CSL shall be applied to important data collected and produced by operators of critical information infrastructure within China, and that for important data collected and produced by other data processors within China, special rules shall be made by the State cybersecurity and informatization department with relevant departments in the State Council. Therefore, data localization remains the default rule for the former category of data. For the latter category, the possibility of cross-border transfer needs to be decided and formulated in future rule-making processes. Despite the lack of more concrete mechanisms for data cross-border transfer, the DSL pledges the Chinese government to "ensure the lawful, orderly and free flow of data"[16] and to "promote the safe and free flow of data across borders" by actively participating in international exchanges and cooperation for the making of international rules and standards on data security.[17] Such undertakings, although largely political rather than legal, suggest a cautiously positive attitude of China toward cross-border data transfers and a more proactive approach to their regulation. Accordingly, China's stance on data localization seems to be more restrained.

[10] PIPL, Article 39.
[11] PIPL, Article 55 (4).
[12] PIPL, Article 40.
[13] DSL, Article 36. The draft version of this provision formulated differently, starting with the requirement of approval and making obligations under international agreements and conventions as exceptions. See Article 33 of the first draft and Article 35 of the second draft.
[14] DSL, Article 48.
[15] PIPL, Article 41.
[16] DSL, Article 7.
[17] DSL, Article 11.

These two legislative moves – i.e., the extraterritorial application of laws and the rules for cross-border data transfers – are indicative of the spatial expansion of China's digital sovereignty, and reflect a nascent, post-CSL regulatory tendency as a result of multiple internal and external factors. To begin with, the data localization rule of the CSL has encountered various criticisms inside and outside of China. Some Chinese scholars comment that the Article 37 of CSL lacks distinction between different data subjects (Cao, 2018, pp. 99–100), fails to meet the requirement of proportionality (Hong, 2017, pp. 59–60), and is unable to balance the two equally important objectives – security and development (X. Zhu & Dai, 2020, p. 87). In the business sector, foreign companies have considered the CSL as a step toward greater trade protectionism and warned the Chinese government that the CSL could further isolate China from the global digital trade (Donnan & Mitchell, 2016). Chinese companies were much less outspoken about their concerns, but it has been pointed out that such strict data localization requirement may trigger protective measures by other countries, impeding the "going-out" of Chinese companies (Liu & Cui, 2020, p. 103). Facing these criticisms, even the Chinese government seemed less ascertain about data localization. Right before the CSL entered into force on June 1, 2017, the Cyberspace Administration of China (CAC) told journalists in a press conference that the objective of the CSL was neither to restrict foreign companies from entering the Chinese market nor to restrict lawful, orderly, and free flows of data. The CAC acknowledged that cross-border data flows had become a precondition for economic globalization and for China's Belt and Road Initiative (Cyberspace Administration of China, 2017). Nevertheless, the blackletter law of the CSL has retained its broad and sweeping phrasing, which continues to be a source of concern for Chinese and foreign companies. The problem of the CSL is partly because the CSL only provides the general structure of cybersecurity, leaving many specific requirements to be fleshed out by complementary laws and regulations in its implementation. However, subsequent implementation and specification of the CSL rules were largely unsuccessful in resolving those concerns and criticisms.[18]

Despite the CSL's formulation, parallel and subsequent regulatory initiatives already pointed toward the direction of extraterritoriality. For example, the Chinese government released several draft guidelines and regulations related to the export of data since the CSL's adoption.[19] In particular, the 2017

[18] For example, in December 2017, the inspection group of law enforcement of the NPG Standing Committee published a report where it admitted that no consensus had been reached regarding the meaning, standard, and determining procedure of critical information infrastructure (S. Wang, 2017).

[19] For example, Measures for the Security Assessment for Cross-border Transfer of Personal Information and Important Data (draft for public comments) was released in April 2017; information security – guidelines for data cross-border transfer security assessment (draft for comments) was released in August 2017; Measures for the Security Assessment for Cross-border Transfer of Personal Information (draft for public comment) was released in June 2019.

draft Guidelines for Data Cross-Border Transfer Security Assessment clearly incorporates extraterritorial application, making, inter alia, "accessibility" of data rather than its physical location the trigger for its application.[20] Considering these pre-existing attempts, the PIPL and DSL exemplify the most recent legislative moves toward extraterritoriality.

Externally, the impact of the US's and EU's regulatory power is undeniable, and superficially, the PIPL and the DSL can be seen as China's emulation of their regulatory models. The US is well known for its extraterritorial laws and the long-arm jurisdiction of its courts (e.g., Putnam, 2016). Its 2018 Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") is an exemplar of the global reach of its sovereign power over data.[21] As for the EU, the General Data Protection Regulation ("GDPR") has become a global model for regulating personal data. China's two legislative moves, particularly with the PIPL, which resembles the GDPR in many respects, may be considered a manifestation of the so-called "Brussels effect" (Bradford, 2020). Indeed, many Chinese scholars recommended to follow the footstep of the GDPR (Shi, 2018; K. Xu, 2019) and legislators admitted that they closely studied foreign and international experiences on data protection when drafting the PIP bill (N. Zhu, 2020). However, China's shift toward gradual extraterritoriality is not a unidirectional imitation of foreign regulatory models; as will be discussed later, this shift will produce geostrategic implications on the emulated regulatory models as well. It suffices to mention here that the emulation of the GDPR by the PIPL is accompanied with caution, especially with respect to the negative effects of extraterritoriality (e.g., the potential trade barriers that other states may put in place in response) and the practical difficulties of enforcement (Liu & Cui, 2020, p. 107). In turn, the PIPL seems to be slightly more restrained than the GDPR regarding extraterritoriality. As we can see, the text of the PIPL makes the intention (i.e., "purpose") of offering products or services to persons in China an explicit criterion for triggering the law's extraterritorial application, whereas the requirement of intention is only mentioned in the GDPR's Recital 23.

In addition to the modeling influence of US's and EU's extraterritorial legislation, it is impossible to overlook the impact of recent mega trade and investment agreements that China has joined. The most notable one is the Regional Comprehensive and Economic Partnership ("RCEP"), which was signed in November 2020 and has accounted for over a third of China's foreign trade in its first year since entry into force (China SCIO, 2023). The RCEP provides a templet of international data governance that contains rules to promote data flows among its members. For example, Article 12.15 of the E-commerce Chapter obliges states not to prevent cross-border transfers of information by

[20] Article 3.7(b).

[21] On this front, it can be argued that the provisions of the PIPL and the DSL on cross-border transfer of data upon foreign authorities' requests are part of the Chinese responses to the US CLOUD Act.

electronic means (Regional Comprehensive Economic Partnership Agreement, 2020). It is true that this rule is followed by a significant list of exceptions, and that compared to the US-led model of digital trade (such as the Trans-Pacific Partnership), the RCEP looks rather unambitious. However, the RCEP remains to be the first significant international agreement that commits China to enhance data mobility across borders. While China's commitment has been interpreted as more symbolic than substantive (Cory, 2021, p. 26), it can still create considerable motivation to speed up domestic legislative process addressing transborder data flows (Li, 2016, p. 781; Gao, 2022). Moreover, China applied to join the Compressive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) in September 2021 (Xinhua News Agency, 2021) and has started adopting CPTPP rules in pilot free trade zones and ports in 2023 (K. Wang, 2023). As the CPTPP has far more stringent rules ensuring cross-border data transfers than those in the RCEP,[22] Xi's gesture may indicate China's moving toward a greater degree of data liberalization, although such liberalization only concerns data related to trade (Gao, 2022). This prospect of greater and freer data flows, however, should not be deemed as a waning of the state's regulatory sovereignty. The deepening of trade liberalization effectively depends on the state's capacity of creating and enforcing legal infrastructures to support and guarantee the operation of the market (Slobodian, 2020; Tzouvala, 2020). Therefore, what may appear to be a retreat of the state's sovereign power is in fact its transformation. When it comes to China, the political will to enhance data mobility goes together with the increased flexibility of the ambit of China's regulatory power over data.

In brief, the recent legislative development in China suggests a revision of the CSL's stricter territoriality. Partially, such a revision is compelled by the economic impracticality of the CSL's sweeping data localization and its enforcement difficulties. It is also caused by a convergence of internal and external incentives pushing for greater data mobility. This revision, however, should not be understood as the weakening of China's digital sovereignty, but rather its adaptation to emerging challenges. The CSL and China's National Security Law remain the basic reference point of recent regulatory instruments, suggesting that the notion of sovereignty is not stepping back but is reinforced through its spatial expansion. As discussed in Section 3.1, such metamorphosis of digital sovereignty is also driven by geostrategic considerations and accordingly will likely have important implications globally.

### 3.2.2 Blocking and Countering Measures and Their Extraterritorial Effects

The second approach, that is, to block or even counter certain foreign measures deemed discriminatory or restrictive against China, can also be found in the PIPL and the DSL. Article 43 of the PIPL provides: "Where any country or

[22] See, CPTPP Articles 14.11 and 14.13 (Government of New Zealand, n.d.).

region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt retaliatory measures against said country or region on the basis of actual circumstances." Similarly, the DSL proclaims that when any nation or region employs "discriminatory, restrictive, or other similar measures" against China "in areas of investment or trade in data and technology for the exploitation and development of data," China may employ "reciprocal measures" against that nation or region based on the actual circumstances.[23] Such provisions certainly make the two instruments an outlier case in current major data regulatory regimes globally. Again, like many Chinese laws, the phrasing remains highly abstract and broad, and relevant guidelines for implementation would be needed to specify key issues, such as how to decide whether a particular measure adopted by another country is discriminatory against China, what "retaliatory" or "reciprocal" measures would be envisaged, or how to determine the target, scope, or severity of such measures.

Irrespective of these details, the two provisions send a clear political signal about China's reaction to the global reach of regulatory powers such as the US and the EU. For instance, with respect to personal data, as the EU has not granted China an adequacy decision, it is fair to ask whether this could be deemed by China as "discriminatory" against China and trigger "retaliatory measures" (Cerulus, 2019). The possibility of retaliation, such as more restrictive market access and data export, could reduce the PIPL's limited liberating effects of cross-border data transfer. While these potentially restricting consequences may lead to data localization or China's self-isolation, such revert is not incompatible with the idea of China's spatial expansion of digital sovereignty, but only one dimension of China's evolving digital sovereignty. In the case of the EU's non-adequacy decision, the potential "retaliatory measures" adopted by China, such as prohibiting data transfers to the EU, would effectively regulate EU-based companies who operate business in China or with Chinese companies, thereby stretching China's sovereign power to what is under the EU's territorial jurisdiction. Hence, the undermining of cross-border data transfers, a form of negative externality, can also be a net result of China's extraterritorial regulatory power.

Compared with the PIPL, the provision in the DSL covers a broader range of measures by foreign countries or regions that could face China's countermeasures, that is, foreign measures regarding investment or trade in data and technology for the exploitation and development of data. This recalls the blacklisting of Chinese tech and telecom companies (e.g., Huawei, ZET, and China Telecom) and sanctions imposed by the US government since the US–China trade war. Elsewhere, India banned Chinese apps including the TikTok for national security reasons. The EU has also begun imposing greater

[23] DSL, Article 26. It's the same wording as Article 25 of the second draft version, which slightly changed the phrasing in the first version from "corresponding measures" to "reciprocal measures."

screening requirements on investments by the Chinese tech companies in the EU market on security ground. In short, all these measures based on national security could possibly be judged by China as discriminatory or restrictive and be responded by "reciprocal measures." An example would be blacklisting certain American or Indian companies to the Unreliable Entity List, which imposes a series of restrictive measures.[24]

Another possible reciprocal measure is provided by Article 25 of the DSL, which says that the state shall implement export controls on data of controlled items for the purpose of protecting national security and interests and fulfilling international obligations. This provision brings to mind the Catalogue of Technologies Prohibited or Restricted from Export, published jointly by the Ministry of Commerce and the Ministry of Science and Technology in August 2020 (PRC Ministry of Commerce & PRC Ministry of Science and Technology, 2020). The Catalogue that includes technologies related to artificial intelligence and data analytics has been widely regarded as a countermeasure to the Trump Administration's TikTok ban by effectively prohibiting TikTok from selling itself to a US company. Again, the negative consequences of such reciprocal measures, such as potential disruptions of global trade and investment that the blacklisting and export control can create, do not necessarily suggest a return to bordered sovereignty based on physical territoriality. Instead, the "other-oriented" character of such tit-for-tat restrictions, based on the self-judgment of whether China is the victim of someone else's wrongdoings, produces extraterritorial consequences affecting foreign actors, effectively subjecting them to China's regulatory power.

In addition to the two laws, the Blocking Rules published by the Chinese Ministry of Commerce on January 9, 2021 is of particular interest. The Blocking Rules applies to

> situations where the extra-territorial application of foreign legislation and other measures, in violation of international law and the basic principles of international relations, unjustifiably prohibits or restricts the citizens, legal persons or other organizations of China from engaging in normal economic, trade and related activities with a third State (or region) or its citizens, legal persons or other organizations (Article 2).

"Blocking" in this document refers to both judicial and political measures, that is, nonrecognition, nonexecution, and noncompliance of foreign legislation or measures identified by the blocking decision made by the Ministry of Commerce.

According to the mainstream interpretation in China, Article 2 means that the Blocking Rules essentially responses to the so-called secondary sanctions of the US (Miao, 2021; Shang, 2021; W. Xu, 2021). In contrast to primary sanctions that prohibit US companies or citizens from doing business with

[24] See, Article 10 of the Provisions on the Unreliable Entity List, released by the Ministry of Commerce on September 19, 2020 (PRC Ministry of Commerce, 2020).

those being sanctioned,[25] secondary sanctions have a much broader scope, covering non-US subjects as well, deterring them from having economic engagements with the sanctioned entities or individuals and therefore are highly controversial (Lowe, 1997; Meagher, 2020, pp. 1005–1006; Meyer, 2008, pp. 926–930). It has been responded to by various third countries adopting blocking statutes to counteract the effects of secondary sanctions. Among them, the EU's Regulation 2018/1100, which was passed after the resumption of the US sanctions against Iran in 2018, has been closely studied in China. Although China's Blocking Rules does not explicitly mention the US, its political gesture is, conceivably, to question the legitimacy of unilateral and extraterritorial economic sanctions imposed by the latter, while providing legal tools for Chinese companies that might be affected by those sanctions.

By opposing the US secondary sanctions, the Blocking Rules also produces extraterritorial effects. Article 2 quoted earlier covers the following two scenarios. First, when China (or specific Chinese companies or individuals) is the target of US economic sanctions (as with the recent Hong Kong Autonomy Act), companies of a third country may decide to cut economic relations with certain Chinese companies in or outside China. Second, when a country other than China (e.g., Iran) is targeted by the US sanctions that apply to non-US companies, Chinese companies may decide to close their business in Iran or terminate contracts with certain Iranian entities in China. In both scenarios, transnational business activities are disrupted by secondary sanctions, and if the Chinese government deems the sanctions as violating international law and basic principles of international relations, the blocking measures could be activated to preserve or restore those business activities between Chinese and foreign companies within or outside the Chinese market.

According to the current texts of the Blocking Rules, we can roughly envisage its operationalization in the following way. For example, the US government decides to impose sanctions on Huawei, prohibiting both US companies (e.g., Qualcomm) and non-US companies (e.g., TSMC, which is Taiwanese) from selling semiconductor chips to Huawei. Facing such sanctions, Huawei reports them to a special working body setup by the Chinese government that would assess the relevant sanctions and decide whether to issue a prohibition order of nonrecognition, nonexecution, and noncompliance. Once the prohibition order is issued, TSMC would be prohibited from complying with the US sanctions and hence should continue selling semiconductor chips to Huawei (while Qualcomm would not be impacted by the prohibition order). If TSMC, caught between the US sanctions and the Chinese prohibition order, decides to comply with the former, Huawei can bring a civil lawsuit before a Chinese court against TSMC for compensation, and the Chinese Ministry of Commerce may also issue TSMC a warning or a fine.

[25] By contrast, the Anti-Foreign Sanctions Law, adopted on June 10, 2021, provides measures countering primary sanctions that directly target China.

In addition to the extraterritorial effects created by "blocking" the extraterritorial reach of foreign legislation or measures, the Blocking Rules has left room for more direct, extraterritorial exercise of the state's sovereign power. According to Article 12, "necessary countermeasures" could be also taken to respond to "unjustified" extraterritorial application of foreign legislation or measures. This reads similar to provisions in the PIPL and the DSL mentioned earlier. The examples of blacklisting "unreliable entities" and adding technologies to the export control catalog are equally relevant here.

It remains to be seen whether "necessary countermeasures" under the Blocking Rules may also take the form of unilateral sanctions by China against a foreign companies or political regime and whether those sanctions may concern companies or individuals of third countries.[26] Similarly, the adoption of the blocking measures provided in the Blocking Rules needs to be specified in practice. Furthermore, given the limited practical effect of the EU's blocking statutes, one may also wonder if the Chinese Blocking Rules would have real consequences on transnational economic activities and on countries imposing unilateral sanctions. Nevertheless, it suffices to say that at this stage, the Chinese government has demonstrated a clear objective of counterbalancing the extraterritorial reach of foreign regulatory powers through the extension of its own. This objective of counterbalancing, also taking into account the provisions in the PIPL and the DSL discussed earlier, is intrinsically tied to the spatial expansion of China's cyber sovereignty.

## 3.3 ANALYSIS: THE INTEGRATION OF GEOSTRATEGIC INTERESTS INTO CHINESE CYBER SOVEREIGNTY

### 3.3.1 An Increasing Integration between Digital Sovereignty and China's Geostrategic Interests

The metamorphosis of China's digital sovereignty can be regarded as both conditioned by and contributing to the so-called "cyber-geopolitics" (An, 2020; Gómez, 2014), by which geopolitical games take a specifically technological turn and data become the main strategic focus. The geopolitical stakes of having extraterritorial power over data and data-related activities and entities become increasingly clear. The examples of countermeasures such as blacklisting foreign companies or imposing export bans discussed earlier demonstrate how the extraterritorial exercise of state power is closely tied to the state's geostrategic interests in an increasingly hostile international

[26] China has adopted the Counter Foreign Sanctions Law on June 10, 2021 (effective on the same day). The two questions, i.e., whether "necessary countermeasures" would involve unilateral sanctions by China and whether such sanctions may concern companies or individuals of third countries, are likely to be answered affirmatively according to this law. Discussing this law is, however, beyond the scope of this chapter.

environment. In addition, the conclusion of the RCEP has been widely interpreted through the geopolitical lens as bringing China enormous geopolitical advantages vis-à-vis the US (Carrai, 2021; Gao & Shaffer, 2021). As these (and future) mega trade and investment agreements create pressure for China to develop regulatory frameworks to enhance the global digital economy, they are also geostrategic drivers shaping the evolution of China's digital sovereignty.

The current cyber-geopolitics that largely started by the trade war with the US has turned into a competition for technological supremacy, as the Huawei sanctions show. The competition for technological supremacy is as much about China's national pride as about the global market share of Chinese tech companies, for dominating the global market help to guarantee a leading role in technological standard-setting that would in turn reinforce the dominance of Chinese companies and technologies in foreign markets. Insofar as the two approaches toward extraterritoriality discussed earlier can be regarded as tools to facilitate the "going-out" of Chinese companies, we can identify a symbiotic relationship emerging between China's digital sovereignty and economic interests of Chinese tech companies: the spatial scope of the former is stretched along with where the latter lies.

This connection between the enlargement of private companies' market share and profits and the extraterritorial spillover of state sovereignty has been examined closely by the scholarship of Marxist and Third World approaches to international law (Anghie, 2007; Chimni, 2017; Parfitt, 2019). From a Marxist perspective, in particular, capital exports are accompanied by capitalist countries' projection of political and military powers overseas; economic competitions between capitalist countries can therefore lead to political competitions, clashes of spheres of interests, and eventually interimperial rivalries (Knox, 2016, pp. 312–315; Miéville, 2006, pp. 227–230). In this sense, the spatial expansion of China's digital sovereignty and regulatory power, as both compelled by and supportive of the market growth of Chinese companies abroad (see Chapter 7), can be seen as demonstrating a rising interimperial rivalry of our time.[27]

Meanwhile, the connection between private economic interests and state sovereignty is particularly pertinent to the Chinese context due to the character of state capitalism that deliberately blurs the line between the public and

[27] One may ask, since data may be argued as "non-rivalrous" (Jones & Tonetti, 2020) and hence fundamentally different from other resources, such as oil, that were objects of historical interimperialist conflicts, whether we can speak about data imperialism and digital interimperialist rivalry. A full explanation would need a separate chapter. It suffices to make two points here: first, the notion of data as non-rivalrous goods is controversial (Rinehart, 2020); second, we may observe both continuities and discontinuities in the transformation of imperialism. What remains central is unequal capacities and distribution of resources to convert data to power (both economic and political) globally. The power dimension of data would make the lens of imperialism highly relevant.

the private interests. This more explicit merge between the public and the private also makes the notion of "digital sovereignty" intrinsically elastic. This elasticity is further reinforced by President Xi's holistic approach to national security, pronounced since 2014 (Xi, 2014). According to this holistic notion, national security integrates multiple elements including "political, homeland, military, economic, cultural, social, science and technology, information, ecological, resource and nuclear security," and has internal and external dimensions. Internally, national security refers to the promotion of development, reform, stability, and safety in China; externally, it refers to the pursuit of peace, cooperation, and mutual benefits with others to build a harmonious world. This all-encompassing notion of national security absorbs China's geopolitical and geo-economic interests, which are by no means purely external – they are intimately tied to domestic factors and produce enormous impact on the domestic economy and politics (Shang, 2021, p. 76). Under this holistic framework of national security, extraterritoriality has been mobilized to stabilize domestic situations (Y. Wang, 2016, pp. 57–58), to empower Chinese tech companies doing business abroad, and to gain China an upper hand in current geopolitical struggles (He, 2019, p. 95; Shang, 2021, p. 76). Either from a Marxist theoretical perspective of interimperial rivalry or focusing on Chinese characteristics of state capitalism and national security, it is not surprising that the notion of digital sovereignty can evolve in a way that blurs the distinction between not only the public and the private but also the domestic and external, projecting China's regulatory power outwardly.

### 3.3.2 Competition and Confrontation through Regulatory Emulation

This spatial expansion of China's digital sovereignty is obviously conditioned by the international environment that China is subject to. In this respect, it is remarkable that the ongoing "cyber-geopolitics" that China is involved in is partly unfolding through regulatory emulation: as discussed previously, both approaches toward extraterritoriality are considerably influenced by the EU's and US's extraterritorial regulations. The connection between geopolitical competition and regulatory emulation is however neither straightforward nor necessary. Putting aside the geopolitical dimension, a more common view in regulation literature is that regulatory emulation can remove regulatory conflicts and contribute to the harmonization of laws (Enriques & Gatti, 2006, p. 961; Lazer, 2006, pp. 460–462; Szyszczak, 2006). For example, the US and the EU, being hegemonic regulatory powers, have created modeling effects that led to a significant degree of global regulatory convergence in many fields, for example, intellectual property, financial regulation, labor, and environment (Braithwaite & Drahos, 2000). Conversely, when sovereigns have "competing regulatory philosophies" (Koh, 2008, p. 16), it has been argued that they can bring about clashes between sovereigns that call for judicial and political solutions. In other words, tensions between regulatory sovereigns are

more often associated with regulatory divergence, and emulation is often seen as one way to resolve regulatory conflicts.

However, the above observation gets much more complicated when (geo) political factors come into play. What China's move toward extraterritoriality by learning from the EU and the US demonstrates is how, in the current geopolitical circumstances, regulatory emulation regarding extraterritoriality can potentially become a tactic by which one polity empowers itself through imitating others to challenge its rivals. This form of regulatory emulation does not solve but rather is likely to perpetuate competitions and even conflicts.

More precisely, the first approach of China's spatial expansion of digital sovereignty may appear as following and contributing to a nascent trend of global convergence for data regulation – convergence in the sense that more and more states (e.g., Brazil, Australia, Canada) start to legislate extraterritorially and design rules for data transfers while strengthening data protection. However, this ostensible trend of regulatory convergence is not just a positive result of "trading up" by competing regulatory sovereigns (Bradford, 2020, pp. 5–6; Vogel, 1995). Rather, such convergence can also be a form of contestation. Take the example of the GDPR, which is often depicted as bringing the "first mover advantage" to the EU in the global regulatory race on the protection of personal data (Smuha, 2021, p. 74), the dynamics of its Brussels effect is not a unidirectional reception of the GDPR's model elsewhere that leads to global regulatory harmonization. The fact that other countries are inspired by and draw upon the GDPR at different degrees can be regarded as precisely the way to mitigate the unilateral global reach of the GDPR. Similarly, the PIPL (together with preceding regulatory instruments on personal data protection) can be considered counterbalancing the EU's role as a global regulatory hegemon.[28]

As for the second approach, contestations caused by regulatory emulation can be much more serious. China's emulation, using mainly the EU's blocking statutes as a model, addresses a particularly confrontational situation, such as secondary sanctions by the US, by reacting with an equally confrontational stance of blocking or retaliation (Huang, Yuan & Hu, 2020). Compared to the contestation in the first approach that still takes place in the broader trend of regulatory convergence, the second approach is explicitly adversarial and may lead to conflict escalation. Given the current international context, the difference between contestations in the first approach and confrontations in the second may likely be more a matter of degree than kind. The slippage between the two situations is reflected by the fact that the PIPL and the DSL contain both approaches. For instance, the respective extraterritorial scopes of the PIPL and the GDPR can create jurisdictional overlaps, which lead to a

[28] Similarly, Chinese scholars have also suggested that the DSL should emulate the extraterritorial scope of the GDPR, shifting the defensive stance of digital sovereignty to a more offensive stance (K. Xu, 2019, p. 59).

regulatory contest; this contest may then be turned into a confrontation where both China and the EU pass normative judgments on each other, leading to the adoption of "retaliatory measures" by China.

In brief, regulatory tensions driven by economic interests (or other normative principles) can slip into geopolitical confrontations, and the likelihood of this slippage is significantly amplified by the emerging cyber-geopolitics, especially since the US–China trade war and the COVID-19 outbreak. In turn, the unfolding of geopolitics can involve the instrumentalization of regulations and regulatory emulations by sovereigns. A common call in China for an extraterritorial regulatory regime for data is precisely based on an acknowledgement that such a regime is necessary to support China in the current geopolitical game where cyber/data security and transnational data mobility are two important levers (e.g., Huang, Yuan, & Hu, 2020).

That regulatory emulation may lead to geopolitical competition is discussed in the general context of tensions China has with the West. Outside this particular rubric of "interimperialst rivalry," what the spatial expansion of China's digital sovereignty can lead to and how "elastic" the spatial scope of China's digital sovereignty can be remain open questions. From a normative perspective that values peaceful coexistence of sovereigns, the openness of these questions leaves room for states' self-restraint and mutual respect and helps to avoid a vortex of tit for tat between rivals. From China's own perspective, the openness of these questions about sovereignty is related to the difficulties peculiar to China that perceives itself as anti-imperial. More specifically, the spatial expansion of China's digital sovereignty, accompanied by the development of extraterritorial legal frameworks, stands in ostensible contrast to China's traditional adherence to the principle of noninterference. The extraterritorial application of Chinese laws necessarily overlaps with and even suspends the jurisdiction of the territorial state. However, given the history of extraterritoriality in China, China has been particularly careful with the wording, avoiding any mention to "治外法权" (the Chinese term for the extraterritorial system created by colonial powers in China since the First Opium War) and sticking to "域外适用" (extraterritorial application, which may sound more technical). This terminological distinction is important for China to not present its expanding regulatory power as imperialist. In addition to the historical factor, there are more practical problems with noninterference. China's extraterritorial jurisdiction over data or data-related entities abroad may trigger objections based on the principle of noninterference by the territorial state. Conversely, if China conceives of certain exogenous economic interests as part of its sovereignty, as the holistic understanding of national security seems to entail, China will logically have no objection for other states to do the same. This means that in cases such as the US applying the effect doctrine to enforce its antitrust law against Chinese companies, China's noninterference claims may be undermined by its own exercise of extraterritorial jurisdiction. Essentially, there will be a growing tension between the principle of noninterference and

China's move toward extraterritoriality to regulate data and data-related entities and activities, both deriving from and justified by the idea of state sovereignty. How to make the two mutually compatible is one of the crucial tasks of defining China's digital sovereignty in an anti-imperialist way. This tension is already displayed in the PIPL and the DSL: while introducing the idea of countering or blocking measures, the two also commit China to international cooperation on data regulation while providing.[29]

## 3.4 CONCLUSIONS

Focusing on three recent regulatory instruments, this chapter identifies an emerging shift toward increasing extraterritoriality in China's approach to governing the cyberspace, data, and data-related activities. This shift is more specifically manifested in two ways: first, introducing extraterritorial rules in data-related legislation and second, authorizing counter or blocking measures against extraterritorial legislation or measures of others. This regulatory tendency indicates a more spatially expansive notion of China's digital sovereignty that evolves in tandem with the growth of profits and global market share of Chinese companies. This more spatially expansive notion also shows the integration of China's geostrategic interests into the notion of digital sovereignty in current international contexts. Furthermore, this tendency is to a certain degree a result of regulatory emulation with the purpose to counterbalance the unilateral global reach of the EU's and the US's regulatory powers.

This tendency toward extraterritoriality is by no means specific to the issue of data governance, since digital sovereignty is closely related to other dimensions of state sovereignty in the Chinese context (keeping in mind also Xi's holistic notion of national security). Therefore, it is not surprising that a more general move toward extraterritorial governing is being conceived of by the Chinese government. Since 2019, the Chinese government started pushing for the establishment of extraterritorial legal frameworks to expand Chinese law's applicability through both extraterritorial legislative and enforcement jurisdictions (Xinhua News Agency, 2019, 2020). The intention, therefore, seems to be not only to facilitate the export of Chinese economy but to export Chinese law more specifically. As a Chinese scholar commented, "the export of Chinese capital will lead the export of Chinese law as a soft power" (Shang, 2021, p. 77). This process of projecting a kind of "Beijing Effect" (Erie & Streinz, 2022) is considered mutually supportive with China's other strategies, such as the Belt and Road Initiative (Shang, 2021, p. 77; K. Xu, 2019, p. 59; Ye, 2020, p. 62).

Despite the increasing motivation and push for extraterritoriality, the expansive notion of digital sovereignty has its own contradictions. As discussed, although China's shift toward spatial expansion is partly conditioned

[29] PIPL, Article 12; DSL, Article 11.

by current geopolitical relations with its competitors, it remains that this shift is at odds with China's traditional anti-imperial and anti-hegemonic posture and its emphasis on sovereign equality. This oddity is also seen in the "Chinese approach" to global internet governance. Termed as "building a community with a shared future in cyberspace" (Xi, 2019), the Chinese approach seems to have a universal pitch, but it reaffirms the principle of respecting sovereignty in cyberspace and condemns "cyber hegemony" (Chinese Academy of Social Science et al., 2020, p. 12). How to have *a* community that is decentered and pluralist is an age-old question, and in the context of this book, this question also involves how to approach diverse, nonstate-centric understandings of digital sovereignty and plural actors claiming digital sovereignty. Yet, a more immediate and practical difficulty for China would be from its own commitment to respecting the sovereignty of other states. As China has traditionally been against the long-arm jurisdiction and unilateralism, how to adapt digital sovereignty to contemporary needs while maintaining internal normative coherence would be a key question.