1

Introduction

Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept

Min Jiang and Luca Belli

1.1 DEBATING DIGITAL SOVEREIGNTY

The last decade has witnessed a series of initiatives, both top-down and bottom-up, in BRICS countries (Brazil, Russia, India, China, and South Africa) to reassert their digital sovereignty, especially in reaction to Snowden's 2013 revelations of US National Security Agency's (NSA's) massive global surveillance programs. Brazil affirmed its commitment to building EllaLink, an undersea cable to connect Brazil directly to Portugal, and connecting by proxy South America to Europe to circumvent US surveillance and enhance its digital sovereignty. Putin's Russia, in a bid to restrict foreign influence and bolster its digital borders, pursued "sovereign RuNet" after passing the *Sovereign Internet Law* in 2019 despite grassroots resistance. In India, besides state-led efforts in constructing digital public infrastructure (DPI) known as the "India Stack," activists organized the social movement #SaveTheInternet in 2016, resoundingly rejecting Facebook's Internet.org initiative (which offers free limited web access to those who cannot afford it) as a form of anticompetitive digital colonialism. China, having long filtered content at the border with the Great Firewall and avowed to defend its digital sovereignty, ramped up its pursuit of digital independence in the unfolding US–China geopolitical rivalry, following Trump administration's ban on Huawei 5G products and threat to force a sale of TikTok to a US firm in 2020 (Jiang, 2021). South Africa, like many other developing countries, tries to forge its own path of digital independence by leveraging Chinese or EU tech equipment, US digital platforms, and its newly enacted data protection policies. Across the five BRICS countries, digital sovereignty discourses, practices, and policies have unfolded differently and unevenly.

This book project, to the best of the authors' knowledge, the first of its kind to explore the digital sovereignty debate in the BRICS countries, attempts to untangle this complex and multifaceted concept from a Global South

https://doi.org/10.1017/9781009531085.002 Published online by Cambridge University Press

epistemic lens. As a hotly debated topic, digital sovereignty inspires interpretive diversity and disagreements rather than uniformity and consensus (Ayers, 2016; Broeders & van den Berg, 2020; Chander & Sun, 2023; Couldry & Mejias, 2019; Couture & Toupin, 2019; Duarte, 2017; Herlo, Irrgang, Joost, & Unteidig, 2022; Kukutai & Taylor, 2016; Mueller, 2017; Pohle & Thiel, 2020). The Westphalian notion of sovereignty – nation-states accorded territorial integrity, legal equality, and noninterference in international affairs monopolize the legitimate use of force and supreme authority over its territory – has not only been challenged in history repeatedly through episodes of colonial expansions and border transgressions (Krasner, 1999) but also faces an unprecedented upset in the digital era from actors ranging from individuals and civil society groups to companies and supranational entities attempting to assert their agency, power, and control.

While the nation-state has traditionally been the legal vessel of sovereignty, chasms exist between normative assumptions of sovereignty and widely uneven practices in reality. Codified into the UN Charter, the modern system of nation-states can trace its origin to the French philosopher Jean Bodin's conceptualization of sovereignty in the sixteenth century as well as the *1648 Peace of Westphalia*, which created a group of legally equal states in the Holy Roman Empire (Grimm, 2015). Yet, centuries of colonization well after the Westphalia treaties and unilateral border transgressions (e.g., invasions of Iraq and Ukraine) call into question many a time the sanctity and normativity of national sovereignty. Besides territorial infringements, asymmetric economic, political, and cultural relations have throughout history produced foreign dominations and interferences. In addition, the normative assumptions of sovereignty also suffer from logical contradictions (e.g., nonintervention versus democracy promotion) and a lack of institutional arrangements to deter dominant actors from abusing their force unilaterally in international conflicts (Krasner, 1999).

Sovereignty is frequently a function of power. Strong nation-states often engage in tactics beyond the scope of their sovereignty normatively defined; weaker states generally lack power and resources to exert effective influence, so much so that Krasner (1999), for instance, argues that sovereignty is "organized hypocrisy." Further, an absolutist notion of sovereignty is criticized to be unattainable, especially in an age of global challenges ranging from organized terrorism, regime change attempts, turbulent international financial markets to global pandemics, climate change, and digital technologies (Havercroft, 2011). In this perspective, the capability to muster digital technologies offers to a wide range of actors a new powerful tool to exercise self-determination,[1] control, and ultimately sovereignty.

[1] The right to self-determination plays an instrumental role to allow individuals to enjoy their inalienable human rights. For this reason, it is enshrined as the first article of both the *Charter of the United Nations* and the *International Covenants of Human Rights*. According

It is important to acknowledge that sovereignty is a complex concept that arose as an attempt to frame the internal structure of a state but ended up becoming the cornerstone of international public law. The German sociologist, jurist, and political economist Max Weber famously considered that states are "political enterprises" (Weber, Gerth, & Wright Mills, 1948), characterized by "the monopoly of the legitimate use of physical force within a given territory" (p. 78). Carl Schmitt (1985), an influential political theorists, argued in line with a Hobbesian reasoning that rather than a monopoly of coercion, the sovereign enjoys the monopoly to decide. In a similar way, Peter Malanczuk (1997), author of one of the most utilized international law manuals, provides a useful discussion of sovereignty, emphasizing that the sovereign enjoys the "supreme power" to decide who is "bound by the laws which he made" and that international law fundamentally interprets sovereignty as independence, stressing that "when international lawyers say that a state is sovereign, all that they really mean is that it is independent, that is, that it is not a dependency of some other state" (p. 17).

These assumptions constitute core pillars underpinning the public law's construction of national institutions and governance based on the consideration of national governments as the only entities able to craft and implement – using coercion, if necessary – their vision for the achievement of the peoples' fundamental right to self-determination. However, these key tenants of public law become considerably more uncertain when they clash with global phenomena and, particularly, digital technologies' capacity to skirt the application of national legislation. This latter dimension means that non-state actors, whether corporations, communities, or individuals, can acquire the

to these international legal instruments, states have agreed that "all peoples have a right to self-determination" and that "by virtue of that right they are free to determine their political status and to pursue their economic, social and cultural development." While self-determination is usually discussed in its external dimension, that is, territorial and political independence from external actors, it is essential to stress that here we are referring to the internal dimension of self-determination, that is, the right to freely determine and pursue one's economic, social, and cultural development, including independently choosing, developing, and adopting digital technologies. Such conception is also corroborated by the fundamental right to "informational self-determination" as an expression of the human right to have and develop a personality, first recognized by the German Supreme Court in the 1983 Census case. The fundamental right to free development of personality is also formally recognized internationally. Article 22 of the *Universal Declaration of Human Rights* affirms that "everyone is entitled to the realization of the rights needed for one's dignity and the free development of their personality." The *International Covenant on Economic, Social and Cultural Rights* consecrates this fundamental principle regarding one's right to education and to participate in public life. Particularly, the *Covenant*'s signatories have agreed that the right to education "shall be directed to the full development of the human personality and the sense of its dignity [...] and enable all persons to participate effectively in society" (Article 13.1). Moreover, the free development of personality is explicitly considered as instrumental to exercise the fundamental right "to take part in cultural life [and] to enjoy the benefits of scientific progress and its applications" (Article 15) (see further elaboration in Belli 2017, 2019).

capabilities to understand, develop, and ultimately exercise agency through technology, thus either eschewing the exercise of the classic state sovereignty or exercising a type of quasi-sovereignty (Belli, 2022).

Drawing from existing scholarship (e.g., Couture & Toupin, 2019; Floridi, 2020), we define *digital sovereignty* as the exercise of agency, power, and control in shaping digital infrastructure, data, services, and protocols. Couture and Toupin (2019) argued that digital sovereignty today is often linked to concepts such as freedom, capacity, nationalism, and increasingly control over data (p. 2310). Floridi (2020) defined digital sovereignty specifically as "the *control* of *data*, *software* (e.g., AI), *standards and protocols* (e.g., 5G, domain names), *processes* (e.g., cloud computing), *hardware* (e.g., mobile phones), *services* (e.g., social media, e-commerce), and *infrastructures* (e.g., cables, satellites, smart cities), in short, for the *control* of the *digital*" (pp. 370–371, italicized in original). Here, we join them in departing from a conventional, normative, state-centric approach that views digital sovereignty as a mere online extension of state sovereignty.

Traditional approaches tend to reify (digital) sovereignty as a self-evident thing while overlooking its often fragile, hybrid, and contested nature. In reality, borders are repeatedly transgressed, and international norms are frequently violated. The gap between the norms of state sovereignty and reality is especially pronounced in the digital realm where much of the world's digital infrastructure, data, and services are overwhelmingly dependent on a handful of Silicon Valley firms and increasingly their Chinese counterparts. By reframing "digital sovereignty" as contested rather than merely accepted, discursively and strategically practiced to articulate legitimation rather than legally binding (Couture & Toupin, 2019; Pohle & Thiel, 2020), we make room for exploring the concept at levels beyond the default plane of nation-states, thus allowing scholars, policymakers, and the public to engage with a wider range of perspectives and discourses on digital sovereignty that can provide visions for the future, especially beyond US and Chinese influence in global digital affairs and governance.

Spanning many disciplines including law, communication studies, political science, international relations, and public policy, the much-debated concept of digital sovereignty is rooted in the classic tension between the supposedly borderless nature of the internet and the bordered conceptualization of sovereign nation-states. At the onset, one must acknowledge the idea of the internet posing unprecedented challenges to state sovereignty is not new (e.g., Johnson & Post, 1996; Lessig, 1999a). Prior works in this area have explored state responses to reassert authority and power in cyberspace (Deibert, Palfrey, Rohozinski, & Zittrain, 2010; Goldsmith & Wu, 2006). However, global digital policymaking was long dominated by an "Internet freedom" agenda (Clinton, 2010a) that regards the internet as a borderless global network, able to circumvent national sovereignty to spread freedom and democracy without paying sufficient attention to the underlying security, economic, political,

and cultural risks associated with such a vision (Morozov, 2011). China's assertion of "Internet sovereignty" (Jiang, 2010), that is, managing networks, information, and population within its borders based on its own laws for security and economic autonomy was scoffed at as an anachronistic, undesirable anomaly, which is understandable due to the Chinese state's instrumental use of domestic laws to implement extensive online political censorship.

In an era of globalization, rather than emphasizing "sovereignty" or "digital sovereignty," scholarly work on digital issues tends to be subsumed under a framework of internet governance or digital governance. Internet governance and digital governance can overlap a great deal, although internet governance tends to stress the governance of the internet itself through a multi-stakeholder model involving states, private sector, and civil society in developing shared principles, rules, norms, and decision-making that shape the evolution and use of the internet (Kurbalija, 2016; WSIS, 2005), while digital governance tends to underscore the use of digital technologies – including those that cannot be properly categorized as internet such as AI – in governing and government processes (Zittrain, 2019). For instance, internet governance focuses on issues such as internet domain names and addresses (Mueller, 2004; Palladino & Santaniello, 2021), internet protocols and applications (DeNardis, 2009, 2014, 2020), and internet governance process and institutions (Mueller, 2017; Palladino & Santaniello, 2021; Radu, 2019). Digital governance, on the other hand, tends to encompass a wider array of digital issues converging with and going beyond internet governance. Earlier works in digital governance tend to be primarily concerned with bridging digital divide (e.g., Norris, 2001), integrating digital technologies to improve public services and democratic participation (e.g., Milakovich, 2012), and balancing privacy and security in digital inclusion (e.g., Chen, 2017). More recent digital governance works focus more on issues of data protection (Chander & Sun, 2023; Cohen, 2019a; Weber & Staiger, 2017; Zuboff, 2019a), artificial intelligence (Crawford, 2020), and quantum computing (Hoofnagle & Garfinkel, 2021). The recent digital governance foci may be connected to the evolution and use of the internet but can also be distinct from it. In both circumstances, their development and regulation may have enormous consequences for digital sovereignty. Thus, digital sovereignty – conceived as the exercise of agency and power in shaping digital infrastructure, data, services, and protocols – crisscrosses internet governance and digital governance.

In the evolution of the digital sovereignty debate, arguably, a critical moment in the digital sovereignty debate came in 2013 with Snowden's revelation of NSA's surveillance programs. Besides a newfound distrust of the US government's "Internet freedom" agenda, US tech giants' catastrophic failures during the 2016 US presidential election also created a deep skepticism of the credibility and neutrality of such corporate entities. These pivotal moments set in motion global repercussions fueling not only critical reflections of our collective digital well-being but also the rise of all forms of "digital sovereignty." Two prominent books – Shoshana Zuboff's *Surveillance Capitalism* (2019)

and Nick Couldry and Ulises Mejias's *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019) that do not address "digital sovereignty" directly – ushered a critical turn in scholarly and public debate of digital governance.

Following the Snowden affair, publications on digital sovereignty witnessed a sharp uptick. A burst of new voices and claims to "digital sovereignty" started to account for the diverse array of perspectives of this concept. Several well-received articles (e.g., Couture & Toupin, 2019; Floridi, 2020; Pohle & Thiel, 2020) have brought the concept to some prominence by repositioning digital sovereignty in a contested discursive field rather than accepting the normative approach to digital sovereignty. In particular, Couture and Toupin (2019) outlined *five* perspectives on digital sovereignty: "cyberspace sovereignty," "digital sovereignty, governments and states," "indigenous digital sovereignty," "social movements and digital sovereignty," and "personal digital sovereignty." Our conceptual framework builds on this line of work while modifying the terminologies and extending it to account for the claims to digital sovereignty made by tech giants as well as supranational entities such as the EU (see "Perspectives on Digital Sovereignty" in this introduction).

To date, focused book-length treatment of digital sovereignty is not abundant, much less from a Global South perspective. In the US, in the aftermath of the Snowden's revelations, there was a renewed emphasis on cybersecurity and sovereignty that produced books such as *Rethinking Sovereignty in the Context of Cyberspace* (Ayers, 2016), an effort by the US Army War College. Scholars such as Milton Mueller pondered on the prospect of a fragmented internet in *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace* (2017). A notable book from China translated also into English – *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace* – was authored by none other than Binxing Fang (2018), an architect of China's now infamous Great Firewall. This book, unsurprisingly, expounds on the Chinese state's official positions. During this period, indigenous studies also contributed to the emerging debate of digital sovereignty through books such as *Indigenous Data Sovereignty* (Kukutai & Taylor, 2016) and *Network Sovereignty: Building the Internet across Indian Country* (Duarte, 2017).

Following EU's enactment of General Data Protection Regulation (GDPR) in 2018, work on digital sovereignty gained further momentum. Scholars in diverse fields such as communication studies, political science, international relations, political economy, and law have contributed to the current debate of digital sovereignty. Relevant books include *Practicing Sovereignty: Digital Involvement in Times of Crises* (Herlo, Irrgang, Joost, & Unteidig, 2022) that showcases a large collection of articles on contemporary digital sovereignty issues, ranging from algorithmic sovereignty and geofilters to feminist approaches and collective sovereignty. Srivastava's *Hybrid Sovereignty in World Politics* (2022) also critiques the normative ideals of state sovereignty

by examining public–private partnerships in structuring sovereignty and international relations in the realms of war, global firms, trade, and international human rights. Most recently, *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Chander & Sun 2023) surveys and debates sovereign states' attempts to cope with the territorial control of data flows and related digital sovereignty issues. New works also pay close attention to individual nation-states' exercise of cyber sovereignty, such as that of China (Kokas, 2022; Timoteo, Verri, & Nanni, 2023).

In sum, our approach to digital sovereignty as the exercise of agency and power in shaping digital infrastructure, data, services, and protocols does not regard the nation-state as the default and only actor capable to exercise and realize sovereign powers. In the digital realm, such powers are often realized through private actors (e.g., tech giants) and desired by individuals, communities, and states that lack them. The shaping of digital infrastructure, data, services, and protocols is thus not only an expression of agency and self-determination but also a product of power and capacity in structuring and influencing digital outcomes. Multiple conceptions of digital sovereignty can overlap or clash as they are experimented with and implemented by different stakeholders in the same jurisdiction. For example, the federal government of a state may implement digital sovereignty policies based on social control through technology (e.g., backdoor mandate), while a local community based in the same state can develop technology for its own collective empowerment (e.g., constructing and managing community networks).

By problematizing "digital sovereignty" and moving beyond a state-centric conceptualization, we can start to raise fundamental questions as to who (legitimately) wields agency, power, and control over digital infrastructure, data, services, and protocols; who ultimately defines "digital sovereignty" and for what purposes; and to what extent a particular form of "digital sovereignty" enhances or worsens the autonomy of, choices by and protection for, a country's citizens. Unlike the freewheeling cyberspace dreamed up by Barlow (1996), we recognize cyberspace is not at all free from states, rules, barriers, prejudices, competing interests, or power differentials. While there is a tendency to frame Western conception of digital sovereignty in terms of public interest and democratic values and conversely brand BRICS promotion of the concept as protectionist and authoritarian, there is also a long history of state surveillance programs in both democratic and nondemocratic countries alike (Chadwick, 2006). While the legitimacy of authoritarian states to exercise "digital sovereignty," for instance to censor, is often called into question, the Snowden revelation of the far reach of NSA and its "Five Eyes" partners into global networks also casts doubt on some Western democracies' legitimacy and neutrality, especially when their actions contradict the purported principles of territorial integrity, legal equality, and noninterference.

If the nation-state is no longer the only legitimate actor with the ability to exercise agency, power, and control in cyberspace or is even capable of doing

so in certain cases, it is then possible and desirable to look past the normative, idealistic, and often mythical state-centric construction of "digital sovereignty" and start to understand, describe, and assess how digital sovereignty is structured in practice. Non-state actors and the exercise of their sovereignty would enter the picture: "corporate sovereignty" embodied by the likes of Google, Facebook, and Amazon whose almighty power easily eclipses those of small nation-states (MacKinnon, 2012); "personal digital sovereignty" grounded in individual rights, autonomy, and freedom in relation to body politics and individual personhood (Koopman, 2019); "postcolonial digital sovereignty" aimed at challenging the violent dispossession of (digital) resources in the process of (digital) colonization (Couldry & Mejias, 2019; Coulthard, 2014); and "commons digital sovereignty" motivated by a desire to create alternatives to state or commercial digital technologies to achieve self-determination and sovereignty of the people through technology managed as a common good (Belli, 2017; Haché, 2017). These diverse ideas challenge the singular, normative assumptions of digital sovereignty centered on the nation-state.

Digital sovereignty thus has multiple, and often, contradictory meanings. Although it is customary to approach "digital sovereignty" from a state-centric perspective, this orthodox approach tends to ignore the alternative perspectives and claims to digital sovereignty made at the grassroots and supranational levels as well as at the intersections between them (Couture & Toupin, 2019). Rather than assuming a state-centric view of digital sovereignty as a given, our goal here is to map the wide range of interpretations of this central concept in the digital era from a BRICS perspective and showcase the plethora of actors – individuals, communities, corporations, nation-states, and supranational organizations – striving to become digital sovereigns rather than digital subjects (e.g., Cheung, 2023).

We also recognize digital sovereignty is often used interchangeably with cyber sovereignty, internet sovereignty, and closely related to data sovereignty. A meta-analysis of these concepts by Hummel, Braun, Tretter, and Dabrock (2021) reveals cyber sovereignty is often evoked by nation-states in the context of cyber defense, while internet sovereignty is more often used to reference power and control over the internet network. We consider data sovereignty a corollary, core concept that undergirds these terms with particular relevance to rights and ownership by data subjects. For us, digital sovereignty provides a much broader frame to discuss the shaping of digital infrastructure, data, services, and protocols.

As our literature review of digital sovereignty scholarship above has shown while there is growing literature on digital sovereignty, there is also a profound lack of literature to address digital sovereignty from a collective Global South perspective, especially grounded in BRICS experiences. Taking cues from such recent work as *CyberBRICS: Cybersecurity Regulations in BRICS Countries* (Belli, 2021b), this project intends to shine a spotlight on how different types of digital sovereigns besides the states are claiming sovereignty and exercising their power over digital infrastructure, data, services,

and protocols in the BRICS countries. While these five developing countries – Brazil, Russia, India, China, and South Africa – are playing an increasingly important role in global digital development and policymaking, their conceptions, narratives, and initiatives of digital sovereignty remain surprisingly understudied as a collective. Contained here is an excellent collection of cutting-edge academic analyses of key digital sovereignty issues in the BRICS countries – ranging from historical imaginaries to up-to-date conceptualizations, from payment systems to smart cities as architectures of digital sovereignty, and from legal analyses to empirical accounts of the exercise of digital sovereignty by states, companies, and communities – offering much needed visibility to frequently neglected perspectives from the Global South.

Much can be gained by bringing varied BRICS digital sovereignty practices under a single umbrella to view how these Global South countries address such challenges separately and together. For instance, although Putin's Russia is known for promoting an ultranationalistic version of "Internet sovereignty" aimed at separating the RuNet from the global internet, it also routinely faces grassroots resistance with individual and collective expressions of digital sovereignty (Daucé & Musiani, 2021). While US tech giants wield immense sovereign-like power across the globe, thus exporting US state sovereignty by proxy (Belli, 2022), they have also been challenged by bottom-up social movements and connective actions (Bennett & Segerberg, 2013) such as India's #SaveTheInternet movement that rejected Facebook's Internet.org initiative seen as a form of digital colonialism (Mukerjee, 2016). China also banned many US tech giants altogether, while investing billions in the development of an indigenous digital ecosystem. The BRICS grouping, although initially an eclectic network of emerging economies interested in multilateral trade, is also increasingly cooperating on digital development and policymaking (Belli, 2021c), taking a loosely coordinated approach in contrast to EU's more uniform supranational stance toward "digital sovereignty" (Leonard & Shapiro, 2020), for instance, through GDPR.

In addition, these BRICS countries present highly relevant and intriguing case studies of digital sovereignty from the Global South with a considerable range. In the BRICS bloc, one finds not only extreme hostile countries such as Russia centralizing its internet control and manipulation in service of its ongoing war efforts in Ukraine but also a tech powerhouse such as China now locked in a new geopolitical rivalry with the US. Besides, India and Brazil – both relatively new democracies with some recent regress in democratic governance – are crucial middle-power countries with the potential to reshape the digital landscape not only in the Global South but also exert influence globally. Finally, South Africa represents a digital arrangement many other countries increasingly find themselves in, that is, relying heavily on China for cheap hardware, the US for applications/software, and its own newly enacted data protection laws to navigate the unfolding digital spaces. Taken altogether, BRICS countries offer a wide range of digital sovereignty policies and solutions from the Global South.

In Section 1.2, we provide an account of why an exploration of the digital sovereignty debate in the BRICS countries is particularly important and relevant at this moment in time. We outline seven major theoretical perspectives on digital sovereignty that serve to elucidate the different digital sovereigns operating on different planes. We close this introduction with a summary for the chapters that compose this volume to recognize their connections and valuable contributions to the digital sovereignty debate in BRICS countries.

1.2 WHY BRICS? RISE OF THE GLOBAL SOUTH AND EMERGING POWER ALLIANCES

Goldman Sachs economist Jim O'Neill first coined the term "BRIC" (O'Neill, 2001) to designate the four largest emerging economies – Brazil Russia, India and China – that experienced a similar phase of development. Geographically dispersed, economically distinct, culturally diverse, and politically different, BRICS countries may not appear to be the most coherent motley crew (Sparks, 2014), especially given the multiple economic, political, and territorial disputes among them, further complicated by the pandemic and the ongoing wars in Ukraine and Gaza. Despite their differences, BRICS nations were united since the 2000s to introduce overdue reforms at Bretton Woods institutions such as the IMF and the World Bank by demanding more transparency as well as more voting power and representation of emerging economies in the global financial system (Stuenkel, 2020). Over the years, the loosely joint bloc did not impose binding conditions on its member states and maintained an informality and a low degree of institutionalization, signaling the bloc's unwillingness to directly challenge the existing US-centered Western global order (Stuenkel, 2020). Rather than being overtly anti-West as Putin's Russia turned recently, most BRICS member states are more "non-Western," in pursuit of support and expanding influence in the existing structure.

Geopolitically, BRICS's emergence represents the "rise of the rest" (Amsden, 2001) in an increasingly multipolar world. The US as the world's sole superpower since the end of the Cold War, suffered a decline in relative power following several pivotal episodes: the highly costly and unpopular wars in Iraq and Afghanistan for two decades since 2001; the 2008 global financial crisis; the pandemic-induced recession since 2020. BRICS countries, on the other hand, include some of the world's largest growth engines (see Table 1.1), representing 25% of global GDP, 42% of the world's population or 3.2 billion (CGTN, 2022a), and 44% of the global internet population[2]. Despite suffering different degrees of economic setbacks exacerbated by the pandemic

[2] Internal issues of some BRICS countries, such as China's aging population and declining birth rate, do pose considerable challenges to their long-term sustainable development (Bai & Lei, 2020).

https://doi.org/10.1017/9781009531085.002 Published online by Cambridge University Press

TABLE 1.1 *BRICS countries profiles (compared to the US)*[3]

	Brazil	Russia	India	China	South Africa	US
Population (2023)	217 million	144 million	1437 million	1425 million	60 million	341 million
Internet Population (2023)	177 million	127 million	692 million	1079 million	45 million	311 million
GDP (2020, USD)	$1.44 trillion	$1.48 trillion	$2.66 trillion	$14.72 trillion	$0.34 trillion	$21 trillion
GDP (2021, USD)	$1.61 trillion	$1.78 trillion	$3.18 trillion	$17.73 trillion	$0.42 trillion	$23.32 trillion
GDP (2022, USD)	$1.92 trillion	$2.24 trillion	$3.41 trillion	$17.96 trillion	$0.40 trillion	$25.44 trillion
GDP per capita (2022, USD)	$8,918	$15,345	$2,389	$12,720	$6,776	$76,399

Sources: WorldoMeter (2023) for population figures, Statista (2023) for internet population figures, World Bank (2022a) for 2020–2022 GDP and GDP per capita figures.

(e.g., China's strict "Zero Covid" policy), the combined GDP of the BRICS at purchasing power parity has surpassed that of the G7 since 2020 (Statista, 2024). BRICS's existence symbolizes a changing global order where the US's relative decline has paved the way for emerging powers such as China, India, Brazil, Russia, and South Africa from the Global South. It is important to pay attention to the emerging power alliances between the BRICS countries and beyond in remaking the global order.

Economically, the BRICS grouping – an unorthodox experiment – is a direct response to the 2008 global financial crisis and the subsequent 2009 Eurozone crisis that exposed the instability of the global financial system centered around the US. The initial BRIC group organized their first informal gathering in 2006. After the 2008 global economic crisis, the BRIC countries whose economies were largely spared from the crises convened their first summit in 2009 with the induction of South Africa in 2010. The grouping's cooperation, cemented by the establishment of the New Development Bank in 2015 with $100 billion initial capital and Contingent Reserve Arrangement, has come a long way. The New Development Bank, conceived not as a rival to established financial institutions such as the IMF and the World Bank, creates a parallel financial system for the developing countries and symbolizes their expectations and aspirations (Economic Times, 2015). In 2021, the New Development Bank added UAE,

[3] Note Russia's economic statistics are subject to considerable variations due to war-related sanctions since February 2022. Russia's federal statistics service announced a 2.1% GDP contraction for 2022, Business Insider reports (Tan, 2023), although World Bank data show GDP growth for the country. Russia's economy has been resilient due to gains in energy prices.

Bangladesh, Uruguay, and Egypt as new members (NDB, 2022). In 2023, the BRICS summit added four more countries – Egypt, Ethiopia, Iran, and the UAE – to the grouping (BRICS, 2023).

It needs to be acknowledged that in the decade and a half since the global financial crisis and especially since the COVID-19 pandemic, many parts of the world including the US and BRICS countries experienced sharp social divisions, economic instability, and widening wealth gaps. A World Bank report (2022b) shows the richest 1% in the world controlled 54% of new global wealth over the past decade. It accelerated to 63% in 2020 and 2021. The top 1% in America, recent research (Smith, Zidar, & Zwick, 2023) finds, owns nearly as much wealth as the bottom 90%. The pattern of widening income gap is also observed in BRICS countries such as China and India (World Bank, 2022b).

In digital matters, during a time of deep economic crisis, widespread social upheaval, and unprecedented nativist furor, the BRICS grouping provides pointers to the future shape of a new global (digital) order. The war in Ukraine marked the most significant military conflict, including cyberwarfare, in Europe since WWII. Except the Putin administration bent on restoring its sphere of influence in the former Soviet states and mounting a direct challenge to the US as a global superpower (Hinck, Cooley, & Kluver, 2019), China and other emerging powers seem more interested in rising *alongside* the US without either assimilating into the current Western-centric global order or directly challenging it (Barma, Ratner, & Weber, 2014). Instead, they have been creating a "parallel order" (Stuenkel, 2016) to accommodate and complement existent international institutions while making more room for their own autonomy and ability to bargain, compete and mitigate risks associated with dependence on external products or services in an increasingly multipolar world. China, for instance, has developed over the last 30 years the only digital ecosystem to rival Silicon Valley's in both scale and sophistication (Miao, Jiang, & Pang, 2021). India has also built a set of DPI widely known as the "India Stack" (Desai, Manoharan, Jayanth, & Zack, 2023; Raghavan, Jain, & Varma, 2019) for identity, payments, and data exchange. While not exempt from criticism, the India Stack offers an alternative framework to the private sector-led platforms created by either the US or Chinese firms (see Chapter 5 for a payment example).

Russia's invasion of Ukraine in 2022 puts its BRICS partners in a difficult bind. The BRICS bloc, notably China, endorses territorial sovereignty. Ten days after the war started, the BRICS-led New Development Bank stopped all new transactions in Russia, signaling its willingness to avert risks (USCC, 2022). Yet, as the war dragged on and motivated by self-interest, the BRICS bloc did not impose on Russia the same sanctions as the US and the EU did, citing NATO expansion as a legitimate security concern (CNN, 2022). Instead, despite some divergent opinions on the war, the group tried to maintain neutrality and continued with the annual BRICS meeting (USCC, 2022). Witnessing the severe economic sanctions the US and the EU imposed on

Russia due to its invasion of Ukraine, in particular the seizing of Russia central bank's overseas assets of $300 billion by the US government, which is not legal by US Treasury Secretary Janet Yellen's own admission (Lawder, 2022), some developing countries are reconsidering their economic, political, and technological alliances in a US dollar-denominated and US dollar-dominated global economy (CGTN, 2022b).

The 2022 BRICS summit reiterated the grouping's commitment for intra-BRICS cooperation focused on sustainable development toward building a global order more favorable to developing countries to address issues including food insecurity, energy shortage, inflation, debt crisis, and de-dollarization (CNN, 2022). After China's successful brokerage of the Iran–Saudi rapprochement, the 2023 BRICS summit further accelerated the expansion of the group under the BRICS+ model by accepting four more countries – Egypt, Ethiopian, Iran, and the UAE – with more to join in the future (BRICS, 2023). The energy-rich bloc – bolstered by Russia, Iran, and UAE – holds considerable sway in global energy and economic affairs.

Ultimately, the war in Ukraine has not changed BRICS countries' trajectory to explore alternative paths for economic and social developments that do not depend on the US-dominated international order that has failed to eradicate – and frequently condoned or produced – gross inequalities, dysfunctional democracies, environmental catastrophes, and persistent militarism. Despite mounting civilian toll, nuclear threat as well as energy, food, and economic crises worsened by the ongoing Ukraine war, the BRICS bloc has moved forward while preserving multilateral and – most importantly – trade relations critical to their own interest and the functioning of their economies and societies (Zondi, 2022).

Seen from a Global South perspective, the BRICS is the latest iteration of a much wider trend toward "South–South cooperation" (The South Commission, 1990). The concept of Global South entails complex layers of geographical, historical, cultural, political, and economic meanings (Lumumba-Kasongo, 2015). While "Global South" traditionally refers broadly to the regions of Africa, Asia, and Latin America as loci of underdevelopment and cultural primitivism in contrast to the "advanced" societies of North America and Europe in a postcolonial sense, the phrase has also signified over time "center-periphery" dynamics in geopolitical power relations (Dados & Connell, 2012). Historically, anticolonial movements have found expressions in the League Against Imperialism begun in 1928 as well as the Non-Aligned Movement started in the 1950s involving 120 countries to counterbalance the US and Soviet power blocs during the Cold War. It was from such historical lineages that one can trace the Group of 77 formed in the 1960s, Group of 15 in the aftermath of the Cold War, and the BRICS after the 2008 global financial crisis (Prashad, 2012). From a postcolonial perspective, BRICS symbolizes a continuation of a centuries' old attempt to challenge and change an unfair system that preserves former colonizers' interests and to gain independence.

Further, beyond the postcolonial lens, the emergence of the Global South, and BRICS in particular, signifies a "*post*global" moment when the world's subalterns recognize the US-led neoliberal globalization experiment as a failed master narrative (Lopez, 2007, p. 1). Instead of seeing globalization and trickle-down economics lift all boats, the last four decades saw the poor, the marginalized, and the disenfranchised bore the brunt of the suffering. Crisis after crisis – from the 1998 Asian financial crisis to the dot-com bubble, from 9/11 to the ensuing 20-year war on terror, from the 2008 financial crisis to the pandemic-induced global recession – traditional Western-led financial and governance institutions, notably the International Monetary Fund and World Bank, are often perceived in the Global South increasingly as barriers rather than propellers of economic and human development. While Russia is not typically considered part of the Global South given its previous super power status and its complicated relations with other developing countries, its membership in the BRICS bloc represents a repositioning of Russia's strategic interest and alliance vis-à-vis the West. It is within such historical contexts that the BRICS have led the search for a "post-Western" model of global governance.

Finally, whether "post-Western" or "non-Western," BRICS' default preference, unlike Russia's in retrospect, is evolutionary rather than revolutionary (Armijo & Roberts, 2014). As beneficiaries of the global system, BRICS members (China and India, in particular) may find it both hard and costly to abolish the existing global order and establish new ones. So, while the then President Trump attempted to weaken the existing rules and norms of the global system including the WTO and Paris climate accord, BRICS member countries have more invested interest in preserving them. Moreover, it seems that BRICS countries', especially China's, vision or capacity to create new systems and institutions such as the Belt and Road Initiative may not only lack intellectual foundation but also face mounting pushbacks and constraints from within the existing system between a rising power and a ruling one (Allison, 2017). Instead, BRICS countries have opted for a type of "competitive multilateralism" (Stuenkel, 2020) that allows them to flexibly choose political and collaborative frameworks to maximize their national interest. Even though BRICS countries may not speak for or represent the diverse voices and regions of the Global South, its emergence and heterogeneity do mark a crucial moment of international development that is worth unpacking and examining.

It is also worthwhile to emphasize the *emerging* nature of global power alliances that the BRICS represents. First, "emerging" suggests that the power alliances are still in the process of formation and there is an open-endedness to it. The BRICS+ model, for instance, developed quickly as six countries got admitted into this new alliance in 2023 with more countries to be added in the near future. Meanwhile, to counterbalance China in the Asia-Pacific, the US has been actively courting India, particularly by forming "the Quad" along with Japan and New Zealand in a new strategic alliance (White House, 2022).

Second, "emerging" indicates that these power alliances in development are relatively new, perhaps different from and not conforming to traditional conceptualizations of the Global South. In fact, scholars such as Acharya (2014) have argued that under the giant tent of the Global South, there are the "Power South" (e.g., China, India) and the "Poor South" (i.e., countries with few resources or little power) at various stages of economic and human development. Stuenkel (2014) also observed that unlike the more inclusive 1955 Bandung Conference or the Non-Aligned Movement that followed, the more powerful members of the Global South such as the BRICS, given their own ambitions for global influence, may not always recognize the challenges of small poor nations or represent their interests.

Should China and Russia be considered part of the Global South? One must admit there is an awkward "in-betweenness" about them. For some, much of China – beyond its first- and second-tier cities – and many of China's population may well qualify as part of the Global South. While China's economic development has lifted 800 million people out of extreme poverty in the last four decades (World Bank, 2022b), 600 million Chinese still live on incomes of barely 1,000 yuan (or $154) per month (BBC, 2021a), and 348 million Chinese on less than $6.85 a day (World Bank, 2022b). On the other hand, as the world's second largest economy with global ambitions, the collective might of China puts it in an emerging superpower category. In fact, the UN's Finance Center for South-South Cooperation (2023) includes 78 countries, but sometimes also label them as a "Group of 77 and China."

Further, Russia is a unique case on its own. Some (e.g., World Population Review, 2023) consider Russia part of the Global North. Others such as the World Bank (2022a) regard it as a mid-tier country between the Global North and the Global South in terms of per capita income. Still others think Russia now aligns itself with the Global South to address grievances with the Global North (Rizzi, 2023). "Emerging" captures the ambiguity of all this.

Finally, such "emerging" power alliances are also an outcome of continuously changing global geopolitics alignments, particularly in the midst of the Ukraine war and conflict over Gaza. The Ukraine war pits Russia against Europe that previously were on relatively cooperative terms over energy imports and exports. As the war unfolded, EU strengthened its transatlantic ties with the US. The Ukraine war also pushed Russia and China – two countries with a complicated history of distrust, competition, and even resentment (Maizland, 2022) – somehow together where the Ukraine war is perceived in both countries now as a proxy war between the US and its biggest rivals. When it comes to the Ukraine war, the Global South is reluctant to pick sides as this war is regarded as a European affair, but whose negative consequences (e.g., energy and food crises) they now must suffer (Tocci, 2023). Similarly, the Israeli-Gaza conflict had major BRICS powers, China and India in particular, gingerly navigate their relationships with Israel, Palestine, the Arab world, Iran, and the West (Burke, 2023). Crucially,

some of the newly admitted BRICS countries, such as Egypt, Iran, and UAE, are playing a major role in these regional dynamics (The Economist, 2023). In this context, a multiplex of new global alliances is emerging to reshape the existing US-centric global order.

1.3 BUILDING DIGITAL SOVEREIGNTY "BRICS BY BRICS"

Just as the BRICS are the developing world's response to the instability and unfairness of a globalized economy, many of the BRICS "digital sovereignty" initiatives are also expressions of a strong inclination to build a multipolar world and seek independence from a US-centric model of digital development and governance, the latter perceived as unfair and unsustainable (Ebert & Maurer, 2013). While "digital sovereignty" is never explicitly mentioned in official BRICS documents, with 40% of the world's population and large sums of one of the world's most valuable resources – personal data (The Economist, 2017), BRICS countries are increasingly leveraging their positions to develop digital technologies, economies, and policies.

Although the "free-flow-of-information" narrative supported by Western countries and championed by the US is appealing, one must acknowledge that global data flows have grown in highly asymmetric fashions. Data has been extracted from Global South countries to generate value mainly in the US while simultaneously rendering the Global South increasingly dependent on technologies provided by a handful of typically US companies. In this context, joint partnerships and activities dedicated to digital affairs and technological cooperation started to appear in the BRICS grouping's strategic agenda over time. Post-Snowden, the 2015 BRICS Summit issued the *Ufa Declaration* to establish a working group on the security of ICT use with the aim "to develop practical cooperation with each other in order to address common security challenges in the use of ICTs" while "sharing information and case studies on ICT policies and programs" (Indian Ministry of External Affairs, 2015).

In the same year, BRICS ICT ministers signed the *Memorandum of Understanding on Cooperation in Science, Technology, and Innovation* to promote digital initiatives such as the BRICS Digital Partnership, the BRICS Partnership on New Industrial Revolution (PartNIR), and the Innovation BRICS Network (iBRICS Network). In 2021, the *New Delhi Declaration* jointly issued at the 13th BRICS explicitly called for – the first time in 15 years – the establishment of "legal frameworks of cooperation" on crucial issues such as "ICTs development and security" (Indian Ministry of External Affairs, 2021). Issues of data protection, cybercrime, content regulation, and e-commerce also received prominent attention.

BRICS's exploration of alternative modes of digital development, governance, and regulation is shaped by several epoch geopolitical events, chief among them: Snowden's 2013 revelations of NSA's global surveillance program, the

vulnerability of democratic infrastructures to social media-enabled manipulation epitomized by the 2016 US presidential election, and Russia's invasions of Ukraine in 2014 and 2022 (and subsequent need to cope with Western-imposed sanctions). While China has been systematically grafting borders onto the internet for decades for fear of a "color revolution," many countries around the world were jolted by these events to move away from a "deterritorialized" view of the internet toward one that is "territorialized" and "sovereignty-minded." Russia's invasion of Ukraine has further prompted the creation of digital curtains on the internet, with the EU requesting to block Russian state media on TikTok, Facebook, and Microsoft (Bond, 2022), and Russia blocking access to Western social media.

As a result, we are witnessing strong currents of territorialization and renationalization of the internet, extending to infrastructure, data, hardware, software, platforms, and tech standards. BRICS countries are no exceptions, although their aims and strategies may be remarkably different. After Snowden revelations, Brazil passed the *Brazilian Civil Rights Framework for the Internet*, or *Marco Civil da Internet*, its first law to create rules and obligations in the internet environment. The Brazilian Central Bank also rolled out Pix quickly in 2020, an instant public payment infrastructure to spur domestic fintech innovations in anticipation of potential foreign dominance (see Doshi & Delgado's chapter). Here, asserting national digital sovereignty is not only compatible with human rights and rule of law but can also enhance participatory democracy. Russia, on the other hand, not only approved data localization in 2015 and the *Sovereign Internet Law* in 2019 but also developed infrastructural capabilities to disconnect the Russian segment of the internet "RuNet" from the global internet (see Chapter 8), which in retrospect appears to be a strategy to build resilience from Western sanctions and to maintain the Russian government's "sovereign" authority (Standnik, 2019).

Following an ambitious Digital India plan aimed at fostering digital inclusion and transformation, India banned zero-rating practices in 2016 on the ground of net neutrality to avoid what is perceived to be a disguised form of digital colonialism (Mukerjee, 2016). Moreover, after GDPR went into effect in 2018, India also passed its landmark Digital Personal Data Protection Bill in 2023 (Indian Ministry of Electronics & IT, 2023) modeled after GDPR and Singapore's data protection law with the intention to continue India's data trade with major countries including the US and Japan (Weymouth, 2023). On the other hand, China elevated "Internet sovereignty" and cybersecurity to a national priority. The Cyberspace Administration of China (CAC), headed by President Xi Jinping himself, was established in 2014. In the same year, CAC inaugurated the annual World Internet Conference held in Wuzhen, China to systematically promote its position of cyber sovereignty and develop international norms. Such high-flying state maneuverings were accompanied by legislative and policy efforts that saw the passage of numerous new Chinese legal regulations aimed at enhancing its cybersecurity and

cyber independence (e.g., Jiang, 2021; Miao, Jiang, & Pang, 2021), including the *Cybersecurity Law* in 2017 as well as *Personal Information Protection Law* and *Data Security Law* in 2021 (Webster, 2023). South Africa, like many African countries, is not self-sufficient enough in technological development, which makes it reliant on US platforms, Chinese tech equipment, and EU digital legislation model, and it is nevertheless designing data protection policies with the unintended effect of increasing state control over private communication (see Chapter 4).

These state-led nation-building efforts, however, are not the only developments that define "digital sovereignty" in BRICS countries, for after all what is sovereignty without the autonomy, choice, or freedom of its own citizens (Fuchs, 2015)? Brazilian users' participation in Mastodon, a decentralized federated social media platform, points to the use of commons-inspired practices of digital sovereignty as an alternative to dominant, privatized, profit-oriented social media (see Chapter 9). In the Russian case, as intimidating as surveillance and censorship may seem, they are never complete with limited spaces for resistance and evasion (see Chapter 8). Often seen as totalitarian by Western observers, the Chinese internet is far from being uniform, obedient, or frictionless. In 2019, for example, a Chinese professor sued Hangzhou wildlife park over facial recognition data collection without his consent, for which the court ordered the park to delete his data and awarded him a partial compensation of $158 (Wu, 2021). Cases as such represent individual and community desires for privacy, autonomy, and self-determination that make up a key part of digital sovereignty discourses.

It is also widely recognized BRICS nations have a highly mixed record of digital authoritarianism and very heterogeneous use of offensive or defensive cyber capabilities to assert sovereignty. While Russia's RuNet goes to the far extreme of "digital isolation" (Sherman, 2021), the Chinese state is known to operate extensive domestic surveillance programs and is frequently cited as a likely originator of many cyberattacks on external targets (Arsène, 2016). Paradoxically, state's political priority mandating firms to maintain backdoors for government access to data for public security also weakens and compromises the development of robust commercial encryptions and data security (Laskai & Segal, 2021). New democracies such as Brazil and India have also experienced notable regress in civil liberties and restrictions of digital rights under Bolsonaro's and Modi's governments (see Chapter 2). South Africa's securitization discourse is similarly worrying for legitimizing state surveillance reminiscent of the apartheid police state (Kuehn, 2018). Far from being an immaculate source of inspiration and emulation, BRICS digital initiatives for online safety and cybersecurity can often seem as pretexts for surveillance and censorship.

Yet the tendency to lump BRICS nations into an authoritarian camp under a "democracy vs. authoritarianism" new Cold War framework is far too simplistic and conflict-prone by assuming Western countries are immune from surveillance

or censorship. Rather, BRICS states' surveillance and censorship practices need to be held in juxtaposition to the grouping's legitimate anti-imperialist, anti-colonial desires, analyzed situationally. Dependence on foreign, especially US, digital technologies, platforms, and services can create and has created conditions of digital neo-colonialism that combines surveillance capitalism (Zuboff, 2019b) and data colonialism (Couldry & Mejias, 2019). The "free" addictive services offered by dominant US platforms are extractive instruments of data mining in building a new form of indentured labor that perpetuates economic and digital dependence (Avila Pinto, 2018). Overtime, "the BRICS grouping is increasingly aware of the economic opportunities brought by digital technology but also that 'free' digital services provided by foreign corporations are not free. They are paid with one of the most precious national assets – i.e. data – and, ultimately, with national sovereignty" (Belli, 2021a, p. 282). Such complex dynamics would not have been captured by an all-encompassing, categorical "democracy vs. authoritarianism" Cold War framework in the digital field.

To further complicate the anti-imperialist, anti-colonial narrative in the digital sovereignty debate are questionable digital practices within BRICS countries and conflicts between them (Fuchs, 2015). While US firms' extractive activities are the subject of postcolonial critique, there is no denial domestic BRICS companies have often benefited from the exclusion of foreign competitors. For instance, not only do large Indian tech companies such as telecom firm Reliance Jio gain valuable access to domestic user data, but data localization measures may well transfer power from foreign tech giants to domestic elites instead of instituting data policies that foster citizens' data sovereignty, as a public good of the people, by the people, for the people (Kovacs & Ranganathan, 2019). Tensions also exist between BRICS partners over their digital policies. China's neo-mercantilist expansion around the world, for instance, has met with both successes and failures (French, 2015). While Huawei and ZTE have offered low-cost, high-function handset solutions to many poor developing nations, Huawei's digital initiatives may well create new forms of digital dependence (see Chapter 7). In a more contentious episode, India banned 59 Chinese apps in 2021 following its border clash with China, with an additional 54 added to the list in 2022 (Reuters, 2022).

Aware of such complex and multifaceted contexts, we argue that the quest for digital sovereignty in BRICS countries to exercise agency, power, and control over digital infrastructure, data, services, and protocols is pursued by a plethora of actors beyond just the nation-states. They include empowered individuals, companies, communities, and even supranational alliances. Rather than following a linear inquiry on a topic as complex as digital sovereignty focused on nation-states only, it benefits to unpack its complexity that unfolds on different planes, in different domains, and across BRICS countries. Doing so will avoid making nation-states the default actors with the legitimacy or capacity to exercise digital power and control over citizens' data and digital lives. As judged by the short yet intense history of the internet, nation-states routinely

fail to protect their citizens' digital rights and aspirations for self-determination. Questionable business players can also drive multi-stakeholder efforts in the name of human rights and democracy while stripping away human protection and dignity. Only by asking to who can (legitimately) wield agency, power, and control over digital infrastructure, data, services, and protocols; who ultimately defines "digital sovereignty" and for what purposes; and to what extent a particular form of "digital sovereignty" enhances or worsens the autonomy, choices, and protection of a country's citizens can we start to have a more meaningful debate of "digital sovereignty."

1.4 PERSPECTIVES ON DIGITAL SOVEREIGNTY

Given the plurality of discourses surrounding "digital sovereignty," we map out here seven major perspectives instead of assuming nation-states are the default and ultimate holders and arbiters of digital sovereignty. Not only does this approach acknowledge the important roles nation-states play in structuring digital infrastructure, data, services, and protocols within their borders, but it also recognizes the complicated realities in exercising digital sovereignty. We include in our conceptual mapping: state digital sovereignty, supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty (see Table 1.2). We recognize various actors – policymakers, technologists, activists, and indigenous and local communities – approach "sovereignty" from highly diverse perspectives with unique assumptions about social justice, autonomy, and governance. In the following, we briefly explicate each perspective, related core concepts, their similarities, and differences as well as their applications in BRICS countries and beyond.

It is worth to note that the applications of these perspectives are highly contextual. For instance, while a BRICS or non-BRICS country's government can pursue state digital sovereignty, it can take different forms (Hong & Goodnight, 2019) – corporate, postcolonial, or commons – depending on the specific circumstances. The US government's laissez faire approach toward digital sovereignty, for example, favors its own tech giants, which in turn extends its structural power globally. While the Indian government initiated the ban of dozens of Chinese apps including TikTok to exercise its state sovereignty to protect domestic internet companies and the data sovereignty of its own citizens, it can also push for the creation and repository of digital public goods among BRICS and other developing countries, a move that aligns more with a commons digital sovereignty framework. Moreover, it is also possible that various civic groups may adopt any of the seven digital sovereignty perspectives outlined including the ones that support or oppose state regulation of cyberspace. In a word, various actors including nation-states may face and adopt different policy choices.

TABLE 1.2 *Perspectives and applications of digital sovereignty in BRICS countries*

BRICS	Theoretical Perspectives	Core Concepts	Applications
Brazil Russia India China South Africa	State Digital Sovereignty	State regulation of digital infrastructure, data, information flow, access, user rights; defense of cyber borders; digital independence; digital nationalism	Data, Algorithms, Undersea cable, Telecom networks (5G), Cloud services, Smart cities, Electronic payment systems, Digital currencies, Social media, Community networks, AI …
	Supranational Digital Sovereignty	Negotiated interdependence between states to assert digital agency, power, and control; framework of digital cooperation; collective state actions and digital cooperation bodies	
	Network Digital Sovereignty	Network interoperability; neutrality of networks; undesirability of state regulation; borderless cyberspace; cryptocurrency	
	Corporate Digital Sovereignty	Laissez-faire, private ordering, and tech giant self-regulation; government regulation as unwelcomed unless it supports tech giants' interests; surveillance capitalism	
	Personal Digital Sovereignty	Informational self-determination, autonomy; individual rights, digital personhood; self-sovereign identity; security and privacy by design	
	Postcolonial Digital Sovereignty	Voice and rights of indigenous peoples; post-colonialism, freedom from (neo)colonialism; access, possession, ownership, control of digital resources	
	Commons Digital Sovereignty	Network self-determination; free and open-source software (FOSS); freedom from corporate and state control; data cooperatives; digital public goods	

We envision the applications of digital sovereignty in multiple and proliferating domains given such domains spread across digital infrastructure, data, services, and protocols: data, algorithms, undersea cable, telecom networks (5G), cloud services, smart cities, electronic payment systems, digital currencies, social media, community networks, AI, and more. It is possible that particular actors may not consider certain domains digital sovereignty-pertinent (*emic* perspective), and scholars and researchers like ourselves may define them as such (*etic* perspective). For instance, we consider India's digital payment system UPI and Brazil's digital payment system Pix as DPIs that can greatly strengthen national digital sovereignty. Yet, they are not labeled as such in India or Brazil.

The application of digital sovereignty within specific domains ranging from data and algorithm to smart cities and community networks also often reflects specific digital sovereignty perspectives. For instance, it is possible to conceive of "data sovereignty" as a domain of national laws and governance structures (Lukings & Lashkari, 2022), thus grounding discussions of "data sovereignty" in a state-centric perspective. However, data can also be regarded as a sphere of individual freedom and personhood (Koopman, 2019) to be protected from state surveillance (Epstein, 2016), making discussions of "data sovereignty" comport with a personal digital sovereignty perspective. Similarly, "algorithmic sovereignty" may regard algorithms as scientific, neutral, and sovereign in their own right, which aligns with a network digital sovereignty perspective. Conversely, "algorithmic sovereignty" can also be positioned to wield corporate power (Jiang, 2014) or become an extension of state oversight of artificial intelligence in the case of China's new registry for recommendation algorithms (Sheehan & Du, 2022). Still others may argue that "algorithmic sovereignty" should be inclusive, transparent, bottom-up, and community-based, allowing communities to exercise agency, power, and control over fundamental digital protocols and infrastructures (Reviglio & Agosti, 2020; Roio, 2018). Given the proliferation of the discourse of sovereignty in many digital domains and applications, even in domains not traditionally thought to be relevant to digital sovereignty such as payment systems, it is key to recognize the particular theoretical perspectives from which actors and interlocutors evoke that carry unique assumptions, biases, and implications.

1.4.1 State Digital Sovereignty

Normative assumptions of sovereignty – territorial integrity, monopolistic use of force, legal equality, and noninterference in international affairs – have been seriously challenged by the advent of the cyberspace (Lessig, 1999a). Over time, however, many governments have reasserted their power (Goldsmith & Wu, 2006). Laws and policies regulating how digital technologies could be used at the national level have been passed since the mid-1990s, implemented through internet intermediaries who act as "points of

control" (Zittrain, 2003) such as operators of national telecom infrastructure, hardware manufacturers, domain name systems, and cloud services. Overall, discourses of state digital sovereignty concern government authority and legitimacy as well as their ability to regulate and control digital infrastructure, data, and users to maintain national laws and achieve autonomy. Whether states can achieve popular sovereignty, or consent of the governed, in the digital realm is an open question (MacKinnon, 2012).

Over the past three decades, BRICS nations have been strong advocates of state digital sovereignty. China was among the first to graft borders back onto the internet in the 1990s through mechanisms such as the "Great Firewall" to filter content and maintain national ownership of digital infrastructure to achieve internet sovereignty (Jiang, 2010). Today, it has the only digital ecosystem that can rival Silicon Valley's, fueled by a degree of technological nationalism to produce indigenous technologies (Jiang & Fu, 2018). China's articulation of cyberspace sovereignty serves as a justification for rejecting foreign interference in its information environment as well as establishing the dominance of party-state ideology and indigenous capacity to innovate (Creemers, 2020; Fang, 2018). In the aftermath of Google's high-profile exit from China, "Internet sovereignty" was adopted as an official state policy by the Chinese government in 2010 to assert control over its infrastructures, information, and population (Jiang, 2021). This approach was further strengthened and promoted abroad by Xi's administration in response to the 2013 Snowden revelations. The "sovereignization" of the Russian internet leveraged the NSA scandal to legitimize the Kremlin's approach to controlling RuNet activities (Nocetii, 2015). Following the passage of *Sovereign Internet Law* in 2019, Russia developed its own technical work-around and alternative version of the domain name system (DNS) in a far more drastic step toward digital isolationism (Sherman, 2021). Brazil not only passed *Marco Civil da Internet* in 2014 and its general data protection law (known as "GDPL") in 2018 but also took concrete steps to construct undersea cable EllaLink connecting Brazil directly to Portugal and by proxy Latin America to Europe to bypass the US surveillance (Yahoo! News, 2022). India started to build a real-time payment system Unified Payments Interface since 2016 (see Chapter 5) to foster a thriving national e-payment ecosystem and has drafted or passed several important data legislations. Post-Snowden, South Africa's digital sovereignty agenda also emphasizes securitization and cyber defense, although such measures also raise concerns for state surveillance and censorship (see Chapter 4).

Besides legislative measures focused on data, state digital sovereignty is often expressed in discourses, projects, and actions of independence that blend into "postcolonial digital sovereignty" (see Section 1.4.5). The colonial legacy in the Global South leads BRICS nations to frequently do so, even though the "state digital sovereignty" perspective is applicable to developed countries too. For example, the Science Council of Canada advocated for "technological

sovereignty" as early as 1967 (Globerman, 1978, p. 43). After Snowden revelations, Deutsche Telekom proposed a "national internet" to bolster Germany's digital independence (Deutsche Welle, 2013). As such, the assertion of state digital sovereignty through legislation, research, and development projects should not be deemed as negative or positive per se merely because it is branded as "digital sovereignty" and promoted by states. The past two decades demonstrate that both legitimate claims and abusive goals can underpin state assertion of digital sovereignty. Ironically, a global internet has not rendered the nation-state or its sovereignty obsolete. Instead, the pendulum is currently swinging toward de-globalization and renationalization of cyberspace.

1.4.2 Supranational Digital Sovereignty

The claim to digital sovereignty, as noted previously, is not limited to the nation-state. Small- and mid-sized countries, in particular, face the perennial challenge of navigating power imbalances (see Chapter 6). The European Council on Foreign Relations, for instance, has publicly endorsed a "sovereign Europe" and "digital sovereignty" strategy to enhance its capacity to act (Leonard & Shapiro, 2020). EU has not only embarked on a legislative restructuring of its digital policies to restrict the undue influence and abuse of dominance by US tech giants and in doing so setting global standards, but it has also teed digital sovereignty and technological strategic autonomy as top priorities (Michel, 2021; Obendiek, 2021).

This European desire harkens back to at least 2005 when a few European nations, led by France, proposed the creation of a Euro-centric search engine to compete against Google and Yahoo!. At the time, former French President Jacques Chirac promised to fund Project Quaero to counter the perceived "threat of Anglo-Saxon cultural imperialism" (Litterick, 2005), although after Germany withdrew in 2006, the project fell apart. Post-Snowden, EU strengthened its data protection by passing GDPR in 2016 and enacting it in 2018, starting to make the "Brussels Effect" (Bradford, 2020) felt around the world. Recently, perceiving EU's lag in advanced digital infrastructure development and deployment (e.g., China–US rivalry in 5G technologies) and digital market (e.g., US dominance in digital platforms and services in EU), EU has passed the Digital Markets Act and the Digital Services Act in 2022 in a bid to further beef up EU's control over its digital sovereignty. Despite national differences and bureaucratic burdens, EU seems committed to maintaining EU values and principles in deploying and creating digital technologies (Obendiek, 2021).

In addition, the world has also moved in a more multipolar direction with the creation of ASEAN in the 1960s, Mercosur in the 1990s, and Africa Continental Free Trade Area in 2019. Developing nations may desire to strengthen their digital policy alignment even though they may not achieve the same level of political coordination the EU seems to have maintained so far.

In contrast to EU's more uniform supranational stance of digital sovereignty as well as growing consensus in OECD countries (OECD, 2022) and ASEAN countries (ASEAN, 2012, 2022) in adopting data-related standards, BRICS nations have only taken initial steps to explore multilateral digital initiatives and cooperation while maintaining their state sovereignty stance. Previously, BRICS summits have issued declarations to address common security challenges in ICT use, promote the global cybersecurity rules within the UN, foster digital development initiatives, and even establish "intra-BRICS" legal frameworks of cooperation. However, concrete multilateral agreements are yet to be hammered out in many areas including tariffs, e-commerce, data protection, cross-border data transfer, technology transfer, cybersecurity, and knowledge sharing (Belli, 2021b; Observer Research Foundation, 2021). To what extent BRICS nations will negotiate between their state digital sovereignty and multilateral digital sovereignty in the bloc remains to be seen. However, should BRICS choose to adopt a set of binding digital agreements, the bloc would hold considerable sway in setting global digital standards and in conducting data trade and e-commerce given it represents more than 25% of global GDP and more than 40% of the world's population.

1.4.3 Network Digital Sovereignty

The romantic idea of cyberspace as a separate space exempted from traditional state jurisdiction, or even a sovereign in its own right, is best embodied in John Perry Barlow's popular manifesto *A Declaration of the Independence of Cyberspace* (1996). His proclamation asserts cyberspace's independence *from* nation-states:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather (Barlow, 1996).

Bold or naïve, the manifesto taps into the public's yearning for freedom and aversion to state control of the new digital frontier. While Barlow seriously underestimated governments' persistent power, the utopian sentiment to reject nation-states in cyberspace lived on. In the essay *Against Sovereignty in Cyberspace*, Mueller (2019) maintains the importance of network interoperability, de-territorialized cyberspace as a global commons, and nonstate governance of the internet (e.g., ICANN) that prioritizes civil society and the private sector. While grounded in understandable and popular sentiments such individual freedom, mistrust of government, and preference for multi-stakeholderism, a weakness of this approach lies in the very flawed international system of asymmetrical power in which global digital governance is embedded. Realpolitik still favors powerful states and their capacity to enforce laws domestically and extend influence extraterritorially (e.g., GDPR's extraterritorial power and

US global dominance through the proxy of its private firms). In retrospect, the internet has long been treated as a medium to socialize, transact, and mobilize rather than as a by-product of a unique stage of capitalism (Cohen, 2019a; Zuboff, 2019a) where essentially a handful of global firms – aided by their governments, mostly the US and China – use it to deploy products and services to create profits and accrue power based on endless extraction, surveillance, and commodification of user data.

It is worth to note the meaning of "cyberspace sovereignty" or "Internet sovereignty" can vary. Barlow's or Mueller's approach evokes a global commons where "states cannot assert sovereignty over cyberspace" (Mueller, 2019, p. 790). The Chinese or Russian use of "Internet sovereignty" notably means exactly the opposite, more akin to the UN-based, state-centric, territorial model (Jiang, 2010) and the "state digital sovereignty" perspective outlined earlier. In theory, national authorities cannot extend control over users, services, applications, or devices outside of their national jurisdiction. In reality, however, state actors such as the NSA or data protection authorities of EU member states acting according to GDPR routinely assert extraterritorial influence. China's latest expansion of its extraterritorial reach through data laws, mirroring the EU policy, attempts the same as EU (see Chapter 3).

1.4.4 Corporate Digital Sovereignty

Exploited by market-centric neoliberalism, the turn from counterculture to cyberculture reimagined Cold War computers as tools for personal liberation, virtual communities as utopian communes, and the digital frontiers as realms of egalitarianism (Turner, 2006). The ascendance of US tech giants since the 1990s and their recent Chinese counterparts birthed a new class of outsized corporate sovereign powers in the digital age. Traditional sovereigns are marked by their authority, legitimacy based on God or law, and supreme power over a territory (Philpott, 2003). These new corporate digital sovereigns (MacKinnon, 2012) have amassed enormous power with little accountability in the digital spaces they create, deriving legitimacy to operate regionally or globally through intellectual property regimes and multilateral trade agreements to wield supreme power over cyberspace.

Tech companies exercise their corporate digital sovereignty through their "structural power" (Strange, 1988) by shaping the functioning of the societies, economies, and democracies through the technologies they provide. Hence, the technological architectures and contractual terms of service they unilaterally define can be seen as the regulatory tools allowing corporate entities to exercise and implement quasi-normative, quasi-executive, and quasi-judicial powers that underpin their corporate digital sovereignty (Belli, 2022).

Corporate digital sovereignty is the by-product of a new era of capitalism: "surveillance capitalism" (Zuboff, 2019a). Unlike industrial capitalism that made commodities out of nature (e.g., real estate), labor (e.g., salary), money

(exchange) (Polanyi, 1980/1944), or post-industrial capitalism that commodified things such as risk (e.g., insurance) and reputation (e.g., PR), surveillance capitalism is based on the extraction, aggregation, and selling of behavioral data and human experiences, often without users' knowledge or against users' interest (Zuboff, 2019a). While corporate digital sovereigns have thrived in a neoliberal environment of free market, privatization, lax regulation, and weak industry self-regulation (Radu, 2019), the tides have turned following the crises of the NSA scandal, foreign interference in the 2016 US presidential election, the Facebook-Cambridge Analytica scandal, and COVID-19 misinformation spreads. US tech giants have been targeted by several regulatory probes (albeit with limited success) and Chinese tech titans have also faced increasing charges of neo-colonialism (French, 2015) and enormous push-backs from the US amid trade wars and geopolitical rivalries between the world's two great powers.

While an increasing number of government initiatives aim at reigning in the excesses of tech giants, especially those based in the US (e.g., EU's GDPR, Digital Markets Act, Digital Services Act), the effectiveness of such initiatives is yet to be seen even though the negative externalities of such firms in multiple areas including taxation, personal data protection, and fair competition have long been well documented. For example, six Silicon Valley giants reportedly created a $100 billion global tax shortfall between 2010 and 2019 by shifting profits from higher-tax jurisdictions to lower-tax or no-tax jurisdictions (Fair Tax, 2019). Despite the recent agreement on a global minimum tax rate of roughly 15% to stop such practices, promoted by the OECD and adopted by the Group of 7 and the Group of 20, taxation of these tech giants has been limited by US government protectionism (Scott & Birnbaum, 2021).

1.4.5 Personal Digital Sovereignty

The claim to personal digital sovereignty – individual exercise of agency, power, and control over personal technologies, data, and personhood (Couture & Toupin, 2019) – has deep philosophical roots. Classical philosophies of individualism affirm the intrinsic value of the individual with precedence over the collective or the state in many modern democratic societies (Swart, 1962). Personal digital sovereignty is also associated with a broad set of civil and political liberties such as autonomy and self-determination that in turn have been appropriated by social and political movements on both the left and the right (Robinson et al., 2017). Moreover, the recent claim to personal digital sovereignty such as the case brought by data activist Maximilian Schrems in the European Court of Justice (Chander, 2020) reflects the backlash against the excesses of surveillance capitalism. Bulk collection of individual data, targeted political ads, and misinformation-amplifying algorithms have not only eroded individual and public trust in powerful states and tech giants but also exposed the limits of industry self-regulation (Cheung, 2023).

Ultimately, personal data – created, collected, and stored on an unprecedented scale in contemporary digitized societies – is always about someone, deeply connected to personhood (Koopman, 2019). Whether a Lacanian psychoanalytic subject or a Foucauldian political subject, the individual has both intrinsic needs and incentives to avoid the Other's excessive gaze to preserve one's privacy, personhood, and control over personal data (Epstein, 2016). This is precisely the rationale behind the formulation of a fundamental right to "informational self-determination" by the German Federal Constitutional Court (1983) in the landmark Census case, arguing this right must be considered an expression of the right to the free development of personality. In this perspective, every individual has not only a legitimate expectation but a constitutional right to exert control over personal data to know what information about him or her is collected, by whom, for what purposes, and with whom it will be shared. As such, any processing of personal data is in principle regarded as an interference with the right to informational self-determination, unless the data subject has consented or the law considers such processing as necessary and proportionate to achieve a legitimate aim.

Similar considerations led the Supreme Court of India to recognize the right to privacy in the landmark Puttaswamy case (Bhandari, Kak, Parsheera, & Rahman, 2017) and the Brazilian Supreme Court to enshrine "informational self-determination" as a grounding principle of the Brazilian data protection law (IAPP, 2020). However, the blurry boundaries between our physical and datafied bodies (van der Ploeg, 2012) as well as the surveillance capitalism logics increasingly jeopardize our autonomy and self-determination. In practice, widespread surveillance exposes the enormous distance between the ideal and the reality of informational self-determination. New discourses and practices of personal digital sovereignty now attempt to bridge the gap through the adoption of technologies, including encryption and free and open-source software and hardware, as alternatives to mainstream applications and services to minimize state or corporate surveillance and manipulation that limit individual choices, agencies, and freedoms (Benkler, 2006; Stallman, 2002).

Users in BRICS countries have been pushing back too, to varying degrees, on both excessive business and state intrusions in their informational self-determination. Whether it is a Chinese university professor suing a local wildlife park over facial recognition data collection without consent (Wu, 2021) or the retired Indian justice Puttaswamy challenging the constitutionality of the Indian electronic ID system "Aadhaar," individual users in the Global South are increasingly resorting to both legal and nonlegal recourses to raise public awareness, change social norms, if not seeking full-scale legislative intervention, to preserve personal digital sovereignty. The demand can also take collective forms as citizens in BRICS countries staged impressive resistance against censorship, surveillance, and shutdowns. Indian farmers protested against agriculture laws and severe internet shutdowns (BBC, 2021b) before winning concessions from Modi government. Chinese users

also successfully pushed back Alibaba affiliate Ant Financial's unauthorized data sharing across Alibaba services and third parties (Wade, 2018).

1.4.6 Postcolonial Digital Sovereignty

Postcolonial thought and discourse have also informed various claims to digital sovereignty made by both indigenous populations and developing countries with colonial legacies. Previously, scholars have explored Australian indigenous data sovereignty (Kukutai & Taylor, 2016) and first-nation Indian network sovereignty (Duarte, 2017). Core issues of sovereignty involving data and network were raised by such works: Australian indigenous people's jurisdiction over data akin to the indigenous jurisdiction over territory, which would confer access, possession, control, and ownership of indigenous people's own data; the deficiency of American Indian tribes to exercise information and cultural sovereignty due to the lack of network infrastructure and indigenous digital content. Echoing the personal digital sovereignty perspective to some extent, this approach seeks a more independent, dignified, and affordable path for indigenous communities to achieve their sovereignty.

Beyond the calls to restore and enhance indigenous populations' agency, power, and control over their own data and networks, postcolonial digital sovereignty discourses also stem from the structural asymmetry and digital divide between developed and developing countries due in no small part to centuries of slavery, predatory practices, and unfair international norms. In various digital technology fields, the relationship between America and the rest of the world has often been viewed as one of center-periphery that replicates colonial relations (Garcia, 2022) through Silicon Valley's digital expansions and endless extractions of user data for profits that perpetuates economic and cultural dependencies. ICANN, initially contracted with the US Department of Commerce and eventually separated from it, was unanimously criticized as an instrument of US domination that often favored industrial and Western interests. While a private sector-led domain name system may seem neutral and convenient, it can continue to serve US interest and its global influence as the American private sector operates as de facto proxy to cultivate "the perception of market-based private ordering" (Bruner, 2008).

BRICS nations' claims to postcolonial digital sovereignty harken back to earlier times such as the Non-Aligned Movement in the 1950s, following decolonization and the New World Information and Communication Order (NWICO) movement in the 1970s and 1980s (see Chapter 2). In the Non-Aligned Movement, countries in Asia, Africa, and Latin America tried to abstain from alliance with either America or the USSR in support of self-determination against colonialism or imperialism. The NWICO debate led by the MacBride Commission was similarly concerned about economic, culture, and media inequality experienced by the Global South as a legacy of colonialism and imperialism (Fuchs, 2015). This form of international alliance of Postcolonial

Digital Sovereignty intersects with other types of anti-colonial efforts by states, individuals, and communities. In recent years, whether it's the Brazilian decision to adopt free and open software (adopted in 2003 by the Lula administration and later abandoned by the Temer administration in 2016), Russia's plan to build digital fences to protect the "RuNet," India's rejection of Facebook's zero-rating service Internet.org, China's adoption of a new Data Security Law, or community efforts in South Africa, India, or Brazil to create their own community networks, post-colonialism and anti-imperialism continue to find new expressions in current times.

1.4.7 Commons Digital Sovereignty

Beyond the postcolonial perspective, commons digital sovereignty – the idea of building digital public goods for digital commons such as FOSS and community networks – tries to transcend state and corporate limitations. In this approach, technologies are developed from and for civil society (Haché, 2017), driven largely not by bureaucratic power or profit but by social movements to create alternative forms of digital sovereignty (Couture & Toupin, 2019). The altruistic motivation draws inspirations from the hacker culture in the 1970s and the FOSS movement, epitomized by the GNU (2022) project launched by Richard Stallman in 1983. The popular Linux operating system, the success of Wikipedia, and growing adoption of Fediverse (Mastodon) for social media are examples of the potential of the FOSS movement (see Chapter 9).

The increasing development of community networks globally including in several BRICS countries – Brazil, India, and South Africa – highlights the evolving nature of new forms of Commons Digital Sovereignty. As crowdsourced collaborative digital infrastructure networks, community networks are quintessential expressions of Commons Digital Sovereignty. They are developed in a bottom-up fashion by groups of individuals, that is, communities that design, manage, and maintain the network infrastructure as a common resource. Thus, the communities and the Commons Digital Sovereignty of their members are the core elements of community networks as they are essential to initiate, maintain, and guarantee the success of such connectivity efforts (Belli, 2017). In fact, community networks are managed according to the governance models established by their community members in a democratic fashion and can be operated by groups of self-organized individuals or entities such as nongovernmental organizations (NGOs), local businesses, or public administrations.

Besides providing access to previously disconnected populations, these networks are particularly interesting as they give rise to an ample range of positive externalities to maximize the network self-determination of large groups of individuals (Belli, 2017). These positive external effects include the construction of new infrastructure with limited investment, the engagement of

locals in the development of new self-governance models, the revitalization of social interactions among local community members and the emergence of new opportunities for accessing information, learning, and creating employment (Belli, 2017).

It is worth to note that the commons digital sovereignty approach – the collective production of digital public goods – is increasingly seen by small- and mid-sized countries as an important strategy to help ameliorate or overcome the dominance of digital superpowers of the US and China. Not only are countries such as France interested in creating new digital commons to avoid the "enclosure" and "exclusivity" of current commercial models (French Ministry of European and Foreign Affairs, 2020), BRICS countries such as India also invest in digital public goods to maximize their autonomy against structural dependence on great powers and their tech giants (see Chapter 6). For instance, starting from 2003, the Lula administration in Brazil forged an alliance with FOSS activists, adopting open-source software as a national policy as a path to digital sovereignty and digital common good (Kim, 2005). The Indian government has used open-source software and DPI in constructing the Indian payment system to leapfrog developed countries (see Chapter 5).

At the BRICS level, the *New Delhi Declaration* (2021), adopted at the 13th BRICS Summit, endorses a commons digital sovereignty approach. In principle, BRICS promotes the use of "innovative and inclusive solutions, including digital and technological tools to promote sustainable development and facilitate affordable and equitable access to global public goods for all" (BRICS, 2021, section 14). In implementation, BRICS line agencies are encouraged to develop a BRICS Platform on Digital Public Goods as a repository for all open-source technology applications created by BRICS members (BRICS, 2021, section 37). For smaller BRICS countries, the creation and repository of digital public goods contribute to "Sustainable Development Goals" that help BRICS and other developing countries to reap the benefit of global digital commons, all the more urgent as seen during the COVID-19 pandemic in distributing vaccines by the increasingly restrictive commercial intellectual property regimes.

The commons digital sovereignty approach may be particularly relevant in an era of billionaire ownership of public utilities, be it Bezos's ownership of Amazon, Zuckerberg's reign at Facebook, Brin's and Page's ownership of Google and Alphabet, or Musk's takeover of Twitter (now X). Overall, the commons digital sovereignty approach – developed by civil society or nation-states in support of this vision – allows for an alternative way to chart the digital future and its governance that is currently dominated by digital superpowers.

1.5 SUMMARY OF CONTRIBUTING CHAPTERS

The book is divided into three segments, bookended by an introductory chapter and a conclusion chapter. The introductory chapter lays the theoretical foundation for the book by disentangling the contesting discourses and

interpretations of digital sovereignty informed by a wide range of literature. The concept of digital sovereignty itself is viewed as a site of power contestation and knowledge production rather than default acceptance. Specifically, seven major perspectives on digital sovereignty are identified from a complex discursive field (see Table 1.2): state digital sovereignty, supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty. The chapter outlines who are actively shaping the definition of digital sovereignty and what perspectives and concepts inform the various discourses of digital sovereignty with what purposes. We also highlight affinities and overlaps as well as tensions and contradictions between these perspectives on digital sovereignty with brief illustrative examples from BRICS countries and beyond. While a state-centric perspective on digital sovereignty is traditionally more salient especially in BRICS contexts, increasing public concern over user privacy, state surveillance, corporate abuse, and digital colonialism has given ascendance to a wider array of alternative perspectives on digital sovereignty that emphasize individual autonomy, indigenous rights, community well-being, and sustainability.

The subsequent eight chapters form the main body of the book, divided into three parts. Part I "State-centric Formations of Digital Sovereignty" recognizes the popular and dominant discourses of digital sovereignty predicated on the nation-state in BRICS countries. This segment includes three chapters: Thumfart's contribution (Chapter 2) that traces the historical imaginaries of digital sovereignty by the Chinese, Russian, and Indian governments from NWICO and WSIS to SCO and BRICS; Cong's work (Chapter 3) that outlines the spatial expansion of China's digital sovereignty in its recent national digital legislations; and Calandro's summary (Chapter 4) of the South African approach toward digital sovereignty caught between securitization and development. Part II "Techno-economic Structurings of Digital Sovereignty" focuses on the implementation of digital sovereignty through technical and financial infrastructures in the BRICS: Hariharan and Natarajan's examination (Chapter 5) of Indian government's open-source digital payment system as an instrument of the country's digital sovereignty; Doshi and Delgado's investigation (Chapter 6) of India and Brazil as examples of "middle powers" with capacity to pursue autonomy and safeguard their digital sovereignty in technical and financial sectors; and Calzati's comparative work (Chapter 7) of Chinese tech giant Huawei's smart city initiatives in South Africa and Italy where corporate digital sovereignty intersects and negotiates with those of the states and local communities. Part III "Grassroots Contestations of Digital Sovereignty" features two chapters: Bronnikova et al.'s examination (Chapter 8) of the Russian public's resistance to the state-imposed "sovereignization" of the RuNet; and Tomaz's study (Chapter 9) of the Brazilian internet activists' discourses and practices in Mastodon, a commons-based alternative to commercial social media networks.

More specifically, Chapter 2 sets the historical context by outlining how China, Russia, and India – three member countries of BRICS and the SCO (Shanghai Cooperation Organization) – constructed imaginaries of "digital sovereignty" since the 1990s. Borrowing the concept of "sociotechnical imaginaries," this chapter examines the regulatory rhetorics, frameworks, and policies employed by the three countries from a state-centric perspective of digital sovereignty. Thumfart argues these sociotechnical imaginaries are centered on protecting national cultural identity, or "cultural sovereignty," against the "free flow of information," a motive that harkens back to the NWICO debates about the imbalance of media and information flows in the 1970s and 1980s as well as the WSIS discussions surrounding digital and knowledge divides in the information society in the 2000s. In particular, he traces the development of these three countries' "digital sovereignty" imaginaries from their unique histories, governing approaches, and global outlooks, whether it is grounded in the Chinese political philosophy of "tianxia" (under heaven), or the "Russian world" to restore Russia's traditional influence on the world stage, or India's anti-colonial tradition coupled with its recent drift toward digital authoritarianism. In the transnational evolution of digital sovereignty imaginaries, the SCO seems to have played a role in disseminating regulatory discourses, norms, and practices from China to Russia and India. Thumfart concludes if BRICS countries are to construct discourses and practices of digital sovereignty beyond US hegemony, they need to consider both the strengths and weaknesses of their approaches grounded often in state-centric and postcolonial claims to digital sovereignty.

Turning to China, Chapter 3 explores the Chinese government's legal strategies to counter EU's and US's regulatory reach and extend its digital sovereignty in cyberspace. Cong argues while China's reterritorialization of its cyberspace is well known, China's emerging tendency to claim extraterritoriality deserves more attention. By closely analyzing recent Chinese legislation – *Personal Information Protection Law, Data Security Law*, and the order by the Ministry of Commerce on blocking unjustified extraterritorial application of foreign legislation and measures, she detects a regulatory shift from territoriality to extraterritoriality. A more spatially expansive notion of "digital sovereignty," her chapter argues, is manifested in two approaches: expanding the territorial scope of application of new data governance legislation as well as blocking and countering foreign measures deemed discriminatory or restrictive against China. Emulating EU and US regulatory approaches, these new measures by the Chinese government either directly expand the legislative jurisdiction or produce extraterritorial effects to protect Chinese sovereignty and interest and to counterbalance the extraterritorial reach of foreign regulatory powers. Taken together, these measures reflect the intricate interaction between China's digital sovereignty and current geopolitical circumstances.

Discussing South Africa, the last country placed alphabetically in the BRICS grouping, Chapter 4 centers on South African digital sovereignty at the

crossroad of securitization and ICT development. It explores South Africa's approach to digital sovereignty by analyzing its digital policies and regulations as well as its posture in the context of globalization. Calandro notes that like many other African countries, South Africa is crafting strategies, policies and rules to frame the increasingly essential role played by ICTs. This process is fraught with tension. On the one hand, South African authorities are struggling to cope with increasing responsibilities of state actors to protect citizens' rights while guaranteeing safety and security online. On the other hand, measures aimed at pursuing public-interest goals, such as data protection and cybersecurity, do not always protect citizens' fundamental rights. Instead, the increasing body of norms, rules, and regulations for the digital space risks expanding state control over private communications, facilitating surveillance and online censorship. In terms of digital sovereignty, he analyzes South African's priorities and positions within the global geopolitical governance of cyberspace, highlights the emergence of a securitization agenda in reaction of cyber threats, and interrogates how policy processes and citizens' rights are impacted by the South African position on digital sovereignty.

Turning attention to economic issues, Chapter 5 explores how the Indian state asserts its digital sovereignty by constructing the Unified Payment Interface (UPI) overseen by the National Payment Corporation of India (NPCI), the latter an entity regulated by the Reserve Bank of India. The case study of Hariharan and Natarajan demonstrates vividly how such indigenous digital payment design, architecture, and governance mechanisms allow for accessible, secure, and interoperable transactions in a mobile-first, open API-based payment network to increase financial inclusion. It also illustrates the need to reduce India's dependence on foreign financial systems, and thus better protected from the shocks that could result from sanctions imposed by foreign states. However, such a system, they argue, is not without potential drawbacks, some of which include the dominance of foreign entities (e.g., Google Pay and PhonePe owned by Walmart/Flipkart) on UPI as well as state-sanctioned monopoly that tends to minimize civil society participation or competition. Besides interoperability and risk mitigation, the authors also advocate a multi-stakeholder governance model for the national digital payment system that bolsters public ownership and institutional checks and balances, a potential model for creating global digital public goods.

Situating Doshi and Delgado's exploration of the digital sovereignty debate in a comparative framework, Chapter 6 considers India and Brazil as examples of "middle powers" and analyzes their capacity to pursue autonomy and safeguard their digital sovereignty. The authors seek to answer two broader questions. First, what agency do middle powers master to safeguard their digital sovereignty. Second, to what extent can domestic politics structure the outcome of this agency. This chapter focuses on the role firms play when great powers weaponize interdependence in finance and digital technology, and subsequently explore the variables along which middle

powers can attain autonomy in the above two fields. The authors contend that middle powers have agency to seek autonomy for themselves and reinforce their digital sovereignty. In particular, data localization policies – structuring jurisdiction over data – play a major role in shaping a country's digital statecraft.

In another comparative chapter (Chapter 7), Stefano Calzati considers corporate digital sovereignty's entanglement with national, and local communities. His discourse analysis of Chinese tech giant Huawei's corporate approach to digital sovereignty in South Africa and Italy highlights its intersections with national (and supranational) digital sovereignty goals and local communities' desire to achieve autonomy and control. Two smart city initiatives – Huawei's OpenLab in Johannesburg and Huawei's Joint Innovation Center (JIC) in Italy – are analyzed to show how the posture of the Chinese corporation can vary according to the national context, thus modulating its impact on the construction of corporate digital sovereignty. The comparative case studies draw from not only the role of China in Africa's ICT development but also the competing visions of internet governance informed by "digital sovereignty" and "data colonialism." Taking a critical approach toward "smart cities," Calzati shows while Huawei partners with local private and public actors in Italy, its initiatives in Africa might frustrate South African authorities' hopes of strengthening national digital sovereignty through integrated local tech initiatives. His analysis reveals digital sovereignty is an increasingly entangled transnational geo-governance issue. Whether tech initiatives foster local digital ecosystems and strengthening local digital sovereignty, or end up creating, reproducing, or reinforcing power asymmetries depends on specific local, national, and international contexts.

In Chapter 8, Bronnikova et al. present the clash between two perspectives on digital sovereignty in the Russian context, namely state digital sovereignty and personal digital sovereignty. The evolution of the Russian government's efforts in implementing the nationalist vision of internet sovereignty runs against an impressive array of civic tactics of circumvention and evasion. Importantly, the chapter notes that the first decade of the twenty-first century has been characterized by relatively high levels of freedom in digital innovation in Russia. Since the early 2010s, regulations aimed at establishing internet sovereignty in Russia have increased as authority of Roskomnadzor, the regulatory body in charge of overseeing media and ICTs, has been substantially expanded. This chapter explores the core elements and limits of Russia's digital sovereignty strategy, which is centered on the "sovereignization" of the RuNet to limit the influence of foreign agents and technology through the implementation of internet sovereignty norms and technical tools. Despite Roskomnadzor's tactics of websites blocking and control of online content through a network of technical intermediaries, activists are continuously learning and using new techniques of circumvention. In the digital sovereignty debate, Russian is highly relevant as it is often deemed a

"laboratory" of broader authoritarian internet "sovereignization" tendencies, thus allowing one to observe and conceptualize the changing patterns in digital policies and politics.

Grounded in a commons digital sovereignty perspective, Chapter 9 documents and critiques the Brazilian FOSS movement through a case study of Brazil's participation in Mastodon, a decentralized federated social media platform. This chapter invites readers to consider and imagine alternatives to corporate digital sovereignty, symbolized by the highly centralized and commercialized tech ecosystem concentrated in the hands of a few Silicon Valley monopolies. As the latest iteration of FOSS activism with regard to social media, Mastodon and the larger project of Fediverse present themselves not only as attempts to develop alternative software and tech ecosystems but also as ambitions to build social movements to transform regimes of intellectual property and surveillance capitalism. While Tomaz remains optimistic about a decentralized, community-driven, privacy-enhanced future, the chapter also cautions against potential pitfalls such as the critical mass needed in user adoption, control over digital infrastructure, persistent digital divide between central and peripheral countries, and power differentiations along racial, class, gender, and organizational dimensions.

The concluding chapter (Chapter 10) acknowledges both the fluidity and the complexity of the notion of digital sovereignty in the BRICS, while also highlighting the necessity of digital sovereignty strategies, policies, and governance mechanisms from a policymaking perspective. The chapter notes that digital sovereignty plays a pivotal role in fostering self-determination, while increasing cybersecurity and strengthening the control capabilities of the "digital sovereign." Importantly, depending on the policy or initiative at stake, the "sovereign" can be an individual, a community, a corporation, or a state. In such contexts, this chapter takes an agnostic approach to digital sovereignty, exploring a selection of practices and providing insight into what this fuzzy theoretical concept means in practical terms. Indeed, digital technologies can facilitate enormous advancements but can also be weaponized against individuals, corporations, and nation-states. BRICS countries' approaches offer some telling examples of how and why the need for digital sovereignty can emerge, but also how confused, and even dysfunctional the implementation of policies aimed at digital sovereignty may become. The heterogeneity and cultural richness of the BRICS is also visible in their approaches to digital sovereignty. Importantly, the differences in their approaches are partly explained by their political stances. Russia and China have played a traditionally antagonistic role to the main digital technology power, the US, and have more structured approaches to digital sovereignty, given the high risks they associate with the lack of such approaches. The other three members of the grouping have less antagonistic but strong historical reasons for being particularly attached to their (digital) sovereignty. These span from post-colonial sentiments to decades of engagement in the

Non-Aligned Movement, to sensitivities raised by recent US abuses of its dominance in digital technologies. Ultimately, BRICS instances illustrate that enhancing a digital sovereign's self-determination, cybersecurity, and control will inevitably reduce the those of other digital sovereigns, likely leading to conflict in the absence of shared and mutually accepted frameworks.

1.6 CONCLUSION

While once imagined as an instrument for a borderless "global village," the internet is currently undergoing complex processes of renationalization (e.g., China, Russia, India) and regionalization (e.g., EU). BRICS countries, like many others around the world, are grappling with conflicting sets of realities and desires: individual privacy and national security, data localization and cross-border data flows, digital independence and international technological trade, often driven by concurrent national priorities, international commitments, and ambitions for global expansion and influence.

This book volume focuses on the central idea of "digital sovereignty" in digital policymaking, disentangles the myriad discourses and interpretations of digital sovereignty, and views the idea itself as a site of power struggle and knowledge production. Toward this end, we mapped out seven theoretical perspectives on "digital sovereignty": beyond the traditional perspective of state digital sovereignty, we extended previous literature to also include supranational digital sovereignty, network digital sovereignty, corporate digital sovereignty, personal digital sovereignty, postcolonial digital sovereignty, and commons digital sovereignty. While the seven perspectives may not be entirely mutually exclusive, they offer analytical lenses to examine the different discourses and approaches toward "digital sovereignty." Rather than viewing digital sovereignty as a mere online extension of a nation-state's sovereignty narrowly defined, this introduction and the subsequent chapters demonstrate that digital sovereignty has become associated with multiple meanings accorded to different agents. It can be appropriated by an authoritarian state or designed for a protectionist agenda, but it can also be used to promote ideals and values rooted in human rights, national development, and community empowerment. The book's concluding chapter will offer more practical examples of and reflections on BRICS countries' digital sovereignty experiences to bookend the effort.

Collectively, we are fundamentally interested in who is actively shaping the definition of digital sovereignty, what perspectives and concepts inform the myriad interpretations of digital sovereignty with what purposes, and how they are applied in a wide range of areas in BRICS countries with what potential impact and challenges ahead. Not only does this collective effort draw on the experiences, practices, and reflections of digital sovereignty from the BRICS scholarly community that contributes to the global conversation on the subject, it also offers a forward-looking take on what a digital world less

dependent on a handful of Silicon Valley or Chinese tech giants might look like in a post-Western world. We believe such an endeavor can help scholars, students, policymakers, businesses, and civil society groups gain interesting insights and perspectives on the conceptualizations, policies, and practices of digital sovereignty in Global South countries. Given BRICS countries' growing international relevance, we hope the perspectives and issues identified in the book project to be of great importance to the future shape and governance of the global digital world.