2

Digital Sovereignty in China, Russia, and India

From NWICO to SCO and BRICS

Johannes Thumfart

2.1 INTRODUCTION

This chapter investigates the sociotechnical imaginaries of digital sovereignty within the BRICS grouping and the Shanghai Cooperation Organization (SCO) with a focus on China, Russia, and India. Sociotechnical imaginaries include a complex network of regulatory, technological, cultural, and societal factors that characterize national approaches to technology (Jasanoff, 2015, p. 4). In addition to the analysis of national approaches, in this chapter, the concept of sociotechnical imaginaries is used to assess approaches characteristic to international organizations.

There is an essential difference between the BRICS and the SCO, the latter originally including Russia, China, and every Central Asian country except Turkmenistan (and today also Belarus, India, Pakistan, and Iran). Broadly speaking, the SCO is focused on regional security and development, whereas the BRICS is focused on global economy and trade. However, in terms of chronology, the SCO preceded the BRICS. When the dialogue between the BRIC countries began in 2006, the SCO had already existed for five years. And since India joined the SCO in 2017, the majority of the original BRICS countries and the most powerful of them are also members of the SCO.

With regard to digital sovereignty within the BRICS countries (Belli, 2021b), the SCO can be considered a forerunner. For instance, the SCO was one of the first international organizations to formulate a comprehensive agreement on information security – *Declaration of the Heads of the SCO Member States on International Information Security* (SCO, 2006). And in 2011 as in 2015, the SCO member states promoted the *International Code of Conduct for Information Security* at the UN General Assembly, which emphasized the "respect for the sovereignty, territorial integrity and political independence

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

of all states, (…) the diversity of history, culture and social systems of all countries" (McKune, 2011). From a critical perspective, the SCO has been characterized as "perhaps one of the most successful examples of multilateral embrace of digital authoritarian norms and practices" (McKune & Ahmed, 2018, p. 3841). In order to conduct an informed debate regarding digital sovereignty within the BRICS, it is therefore highly relevant to analyze the position of the SCO and its leading nations: China, Russia and India.

This chapter demonstrates how the sociotechnical imaginaries of digital sovereignty in China, Russia, and India are related to the much earlier conception of "cultural sovereignty," which was developed at the New World Information and Communication Order (NWICO) debates at UNESCO in the 1970s and 1980s. This conception, in turn, influenced particularly the Chinese discourse of "information sovereignty" in the late 1990s, from where the idea spread to the SCO and to Russia and India.

Starting from this genealogy, this contribution makes the case that, intertwined with economic and geopolitical factors, the sociotechnical imaginaries of digital sovereignty in China, Russia, India, and within the SCO and later the BRICS are centered around the idea that it is necessary to protect national cultural identities against the "free flow of information" enabled by digital networks, which has both domestic and international aspects dimensions. This, of course, has problematic aspects. Although the tendencies of monopolization of global communication and the concomitant uniformization of global culture regularly draw criticism, these imaginaries of digital sovereignty often serve as a means to justify practices of censorship and, in particular, obstacles to transborder information access, which violate Article 19 of the *Universal Declaration of Human Rights* (UDHR) that includes the right to "receive and impart information and ideas through any media and regardless of frontiers" (Universal Declaration of Human Rights, Article 19).

Section 2.2 includes a brief definition of digital sovereignty. The subsequent sections follow a chronological order. Section 2.3 proceeds with an analysis of the paradigm of the free flow of information and the postcolonial NWICO debates at UNESCO (the late 1970s to the early 1980s). In Section 2.4, I will lay out how these debates influenced the Chinese imaginary of digital sovereignty in the late 1990s and how China promoted its ideas, for example, within the World Summit on the Information Society (WSIS) from 2002 to 2005. In Section 2.5, I will focus on the SCO itself, which appears to have served as one transmission belt to export the Chinese imaginary of digital sovereignty to other countries, most notably Russia. In Section 2.6, I will lay out how cultural issues matter to Russia's "sovereignization" of the internet from 2011 on and how the country's specific sociotechnical imaginary of the "sovereign internet" was constructed. In Section 2.7, I will show how the SCO-member India (since 2017) developed a semi-authoritarian imaginary of digital sovereignty closely related to cultural issues, most notably regarding

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

the Hindu nationalist government's internet shutdowns. In the final part, I will discuss these findings in relation to BRICS.

2.2 DEFINITION OF DIGITAL SOVEREIGNTY: A NOT-SO-NEW ALIGNMENT

Concepts related to digital sovereignty are part of a whole group of comparable, yet not identical concepts: technological sovereignty, information sovereignty, cyber sovereignty, internet sovereignty, data sovereignty, souveraineté numérique, soberania digital, digitale Souveränität, 网络主权 ("network sovereignty"), 信息主权 ("information sovereignty") and Суверенный интернет ("sovereign internet") (Thumfart, 2022).

While these terms can, by no means, all simply be equated, they all can be used, often by national governments, to signify the idea of national control over digital phenomena. In almost every case, this includes the concept to "align" (Mueller, 2017) cyberspace with territorial borders, which has also been described as the "territorialization" (Lambach, 2020) or "sovereignization" (Shcherbovich, 2021) of cyberspace.

In the contemporary debate, digital sovereignty has become a buzzword. What distinguishes digital sovereignty in comparison to, for example, data sovereignty, information sovereignty, or cybersecurity, is its vast scope. Information ethicist Floridi (2020) defines the term as including control over data, software, standards, processes and protocols, hardware, services, and infrastructure. Corresponding to this wide scope, the agenda of digital sovereignty includes policies such as data localization, internet censorship, the nationalization of digital infrastructure, and the construction of cyber capacities. While Floridi and many others (including Jiang and Belli in this volume) make the case that digital sovereignty can also be attributed to individuals, companies, and supranational entities, I am focusing here on digital sovereignty understood as an attribute of nation-states.

From the perspective of the Global North's developed countries, the shift from the unregulated internet to digital sovereignty with increased state regulation of the digital has been primarily owed to the catalytic events of the 2013 Snowden revelations, the Facebook–Cambridge Analytica scandal during the US presidential election and Brexit in 2016, and the disinformation crisis during the Covid-pandemic in 2020 and 2021 (Thumfart, 2022).

However, as I have argued elsewhere, discourses related to digital sovereignty have a far older history outside of the West. Western conversion to this norm is a comparably recent phenomenon that rather universalizes digital sovereignty than constituting a new invention (Thumfart, 2022). In this sense, the discourse around digital sovereignty is exemplary for the dawn of a truly multipolar world, in which the developed countries of the Global North are no longer exclusively setting the agenda (Thumfart, 2024b). This contribution

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

reconstructs the pre-history of the current debate about digital sovereignty from a decidedly non-Western perspective.

2.3 THE FREE FLOW OF INFORMATION AND NWICO (FROM 1944 ON)

The central idea opposing digital sovereignty is the paradigm of the free flow of information as institutionalized in the UNESCO constitution (UNESCO Constitution 1945, Article 1.2). This paradigm is particularly interesting within a BRICS context, because it is closely connected to the debate about access to colonial and postcolonial media markets. The origin of the free flow of information paradigm predates digital technologies. Around the end of WWII, US officials criticized European powers' grip on the informational infrastructure and markets in their colonies and demanded equal access (Schiller, 1975).

For example, in 1944, the chairman of the US Federal Communications Commission criticized that "Great Britain owns the major portion of the cables of the world" and condemned this "control of communication facilities by one country with preferential services and rates to its own nationals" (Schiller, 1975, p. 77).

In 1946, the US Assistant Secretary of State outlined the government's position, which was, at that time, not directed against dictatorships, but rather against European geopolitical competitors.

> The State Department (…) plans to do everything within its power along political or diplomatic lines to help break down the artificial barriers to the expansion of private American news agencies, magazines, motion pictures, and other media of communication throughout the world (…). Freedom of the press – and freedom of exchange of information generally – is an integral part of our foreign policy.

The US ambition was ultimately successful. The European powers were weakened by WWII and willing to cooperate due to their fear of the Soviet Union (Schiller, 1975). The US's position regarding information freedom influenced UNESCO's position on this matter, which included the free flow of information in its charter (Schiller, 1975, p. 79). As mentioned in the introduction, this is also backed by Article 19 of the UDHR, which includes the right to access information across borders through any media.

However, with decolonization movements from the 1970s to the 1980s, leading governments of the Non-Aligned Movement, India, Cuba, and Tunisia, supported by the Soviet Union and China, began to criticize the unidirectionality of the global information flow from the developed countries of the Global North to the rest of the world (Bhuiyan, 2014, p. 4). During the debates on the NWICO at UNESCO, these countries demanded restrictions to the free flow of information based on "cultural sovereignty," which is, in many ways, the origin of today's debate on digital sovereignty (Carlsson, 2003).

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

This agenda had clearly an economic aspect, as it was part of the wider concept of the New International Economic Order (NIEO). However, the main argument in the NWICO's conclusive report is that information cannot be a commodity as any other since it is the very foundation of society and, thus, inherently political: "Information is a service that must exist before commodities in general can be produced and exchanged. These considerations ought to act as a corrective to the transformation of information into a simple commodity" (MacBride & Commissioners, 1980, p. 153).

Further, the report argues that the diversity of cultures is threatened by global "assimilation" to a dominant global culture (MacBride & Commissioners, 1980, p. 31). The report sketches "cultural sovereignty" as a means to prevent such a decline of cultural diversity. However, the text also stresses that cultural sovereignty cannot be understood in a too simplistic, essentialist manner (MacBride & Commissioners, 1980, p. 161) and that it could be abused to justify the violation of human rights (MacBride & Commissioners, 1980, p. 189), for instance, regarding the freedom of expression and minority rights.

It is noteworthy that the NWICO debates included all of the original BRICS countries. However, the debates ended in the early 1980s due to, among other reasons, the fact that these proposals undermined the communication hegemony of both the United States and Great Britain who withdrew from UNESCO in 1984 and 1985 respectively.

Instead, the doctrine of the free flow of information prevailed. During the late 1980s, it became increasingly political. This was owed to the fall of the Soviet Bloc in 1989, during which the free distribution of information by dissidents played a crucial role. The experience of the end of the Cold War led the US to believe that the free flow of information was desirable because it inherently promoted democratization (McCarthy, 2015, p. 84). A particularly clear expression of this idea is an essay by Bill Clinton's foreign policy advisor Joseph Nye and US navy admiral William A. Owens from 1996, titled "America's Information Edge" published in *Foreign Affairs*. It reads:

> The beauty of information as a power resource is that, while it can enhance the effectiveness of raw military power, it ineluctably democratizes societies. The communist and authoritarian regimes that hoped to maintain their centralized authority while still reaping the economic and military benefits of information technologies discovered they had signed a Faustian bargain (Nye & Owens, 1996, p. 35).

The idea that the free flow of information inevitably democratizes societies corresponds to the "Internet dictator's dilemma" (Boas, 2000), which conceives of digital technologies as forcing authoritarian States into accepting freedom of expression and democratic participation. During Hillary Clinton's tenure as the US Secretary of State, this idea was reframed as the "Internet Freedom" agenda (Clinton, 2010a).

Although there were occasionally debates in the developed countries of the Global North regarding the harmful side of the free flow of information

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

(e.g., on drug trade and child pornography), the issue of whether the free flow of information threatens national cultures and how this could be a political problem has rarely been addressed in the Global North. Different from a time when the Global North's hegemony was practically unchallenged, today's discursive landscape in the Global North includes extensive discussions of the problematic impact of disinformation on deliberative processes in liberal democracies, particularly disinformation that originates from hostile geopolitical rivals (Thumfart, 2022).

2.4 THE ORIGINS OF DIGITAL SOVEREIGNTY IN CHINA (1996–2015)

Inspired by the NWICO debates, the Chinese sociotechnical imaginary of digital sovereignty that focuses on national control over digital technologies first appeared during the 1990s (Cong & Thumfart, 2022). It is determined by five factors of cultural and political nature.

First, this development is owed to the fact that with the fall of the Soviet Union, China began to emerge as the US's main geostrategic and economic rival, a role that it even played in its domestic political imaginary before it was perceived as such in the West. In this context, the Chinese government was and is focused on defending itself against the possibility of regime change from abroad through the means of digital communication.

Second, this geostrategic rivalry is connected to a cultural and historical issue. Since China conceives of itself as a post- and anti-colonial power, it is, in principle, vigilant regarding any developments coming from the US as the global hegemon. This anti-colonialist national imaginary was particularly influential during the 1990s, which saw the return of Hong Kong (in 1997) and Macao (in 1999) and a popularization of anti-colonialism in computer games and movies (Sly, 1997).

Third, the non-liberal and socialist country knows no strict separation between the private and public sectors. Instead, it seems rather natural to put digital technologies under state control. This is informed by Marxist political economy, which prescribes an active role of the state in promoting and controlling new technologies.

Fourth, China's understanding of its sovereignty over digital communication is informed by Confucianism, which became very important with the rehabilitation of traditional Chinese culture under Deng Xiaoping (Jiang, 2010). In order to assess the impact of Confucianism, it is crucial to stress that China, although being officially atheist, cannot be considered a secular society according to European standards because secularization was a result of specific confessional conflicts in sixteenth- and seventeenth-century Europe. And, accordingly, Confucianism is neither a religion nor a secular philosophy in the Western sense. Rather than recognizing the independence of the religious or cultural sphere, Beijing understands religious and cultural

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

traditions as means to achieve the wider aim of a Confucian "harmonious society." This is exemplified by Beijing's authority over the recognition of reincarnated Buddhist lamas (Szonyi, 2009). Accordingly, while imported from the modern Western legal tradition, the Chinese understanding of sovereignty is informed by a Confucian and imperial tradition that is characterized by a universal understanding of sovereignty according to a system 天下 (*Tianxia*, lit. "under heaven") (Coleman & Maogoto, 2013; Zhao, 2019). This holistic, all-encompassing understanding of the state is a crucial element of Chinese political ideology and leads to the idea that cultural issues are inherently political.

Last but not least, China's vigilant stance against US digital hegemony also stems from the fact that the domain name system, a core architecture of the internet based on the Roman alphabet, manifests Western cultural hegemony. It took until 2009 that the Internet Corporation for Assigned Names and Numbers (ICANN) globally approved the creation of internationalized country code top-level domains. In line with worldwide concerns regarding this issue (Baasanjav, 2014), Chinese scholars in the 1990s and early 2000s saw the predominance of the English language on the internet as a threat to their cultural identity (Gong, 1998; Han, 2000). The Chinese government was so concerned with this problem that it introduced domain names in Chinese characters independent from ICANN as early as 2000 (Baasanjav, 2014, p. 996).

The Chinese position on issues related to digital sovereignty was formulated by Chinese scholars from 1996 on (Cong & Thumfart, 2022). It was expressed in the most poignant way in an essay from 1998 written by Gong Wenxiang of the School of International Relations at Peking University on "information sovereignty" (信息主权) (Gong, 1998). First, the essay explicitly refers to the NWICO debates. Following the arguments employed there, it criticizes US cultural domination and argues for "the establishment of equal, just and mutually beneficial communication." Constructing a fundamental conflict between the notion of "information sovereignty" and the "globalization of communication and information," the essay states:

> The so-called 'Coca-Cola culture', symbolized by rock music, MTV etc., has long been popular all over the world, and several major news agencies, such as AP, Reuters, BBC and CNN, have dominated international news dissemination. In the last instance, cultural communication and journalism are all about values that affect and influence the lifestyles and ideologies of their audiences. National information sovereignty (信息主权) should include the right to develop and consolidate national ethos and national culture through national and international dissemination of information (Gong, 1998, 42f.).

Employing a more aggressive tone, the essay underlines the strategic origins of the internet itself in the US ARPANET. In this context, the essay highlights the tactical significance of IT infrastructure and refers to the US's use of EMP-warheads during the first gulf war in 1991. It concludes:

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

> From CNN's exclusive field reports to the use of advanced automated weapons, the United States presented the world with a new type of warfare, which foreign scholars called 'information media warfare.' According to experts, the important aspect of warfare in the next century will be information warfare: digital information weapons such as computer viruses, logic bombs, and long-distance telephone network jamming devices are the nuclear weapons of the 21st century (Gong, 1998, p. 44).

Drawing from the Confucian philosopher Mencius, reflecting on the Opium War and the Boxer Rebellion, the essay explicitly discredits the notion of the free flow of information as an ideology that serves the interests of Western "information superpowers": "Whilst the information superpowers sing the hymns of 'international freedom of communication' and 'information without borders,' many developing countries feel that their rights are being taken away and even their national security is being threatened" (Gong, 1998, p. 45).

Gong Wenxiang's (1998) essay and similar ones on 网络主权 ("network sovereignty") and 网络殖民主义 ("network colonialism") illustrate the intellectual historical background that predestinated China for being the first country to explicitly develop concepts related to digital sovereignty (Cong & Thumfart, 2022; Guan, 1997; Tang, 1998). On several occasions, the NWICO debates are explicitly cited as a blueprint for the Chinese approach of digital sovereignty (Cong & Thumfart, 2022).

The following practical and intellectual development of these ideas in China has three aspects: First, a cultural aspect; second, a security aspect; and third, an agenda related to global internet governance. The SCO, which will be discussed in Section 2.5, is part of all three aspects.

Cultural issues played a role both externally and internally. State control over internet content through censorship intensified in China in 1999 with the persecution of Falun Gong, which was considered a sect with political ambitions by the Chinese government. The group had been very active online, communicating through its international network, foreign servers and foreign websites to circumvent censorship by the Chinese government. In June 1999, the infamous 610 Office was established to crack down on this group through means including blocking access to the group's sites outside China, undertaking cyberattacks against the group's websites in the US, Canada, and Australia and requiring the registration of all encryption technology used by private entities and individuals (Chung, 2002, p. 96). This conflict acted as a crucial catalyst in the successive development of the "Great Firewall" that started to block content beyond Falun Gong, for example, the cause of Tibetans or Uyghurs or the events of June 1989 (Creemers, 2020, p. 13). It is obvious that the question of minorities within China is not only a political issue but also a cultural issue, particularly important from the perspective of the Chinese holistic and not necessarily secular (in the European sense) understanding of the state. These cultural aspects are not merely restrictive and top-down but have a productive and bottom-up element. They are reinforced by a form of "digital nationalism" in Chinese civil society (Schneider, 2018).

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

Beyond these cultural issues, security concerns played a role in the development of Chinese concepts related to digital sovereignty. One of the better-known outcomes of this discourse is an essay by the influential flight engineer Ji Zhaojun published in 2000. This essay "Network Security, Sovereignty, and Innovation" compared digital sovereignty to sovereignty over airspace and maritime space and promoted the idea that open digital networks further US dominance (McKune & Ahmed, 2018, p. 3838). In 2004, Chen Xueshi of the National University of Defense Technology affiliated to the People's Liberation Army defined national "information borders," which has since then been a characteristic feature of the Chinese discourse (McKune & Ahmed, 2018, p. 3838).

Third, China promoted concepts related to digital sovereignty in international fora of global internet governance, making it a prime norm entrepreneur in these contexts (McKune & Ahmed, 2018). Take as an example China's engagement in the World Summit on the Information Society (WSIS), ICANN and the International Telecommunication Union (ITU), the SCO, and the World Internet Conference (Negro, 2020).

China has had a presence at ICANN since 1999 and it demanded a reform of the ICANN multistakeholder system in favor of an UN-like, state-centric mode of control as early as 2002 (Arséne, 2015, p. 29). The country found its allies on internet governance in the first phase of WSIS that year (Negro, 2020, p. 8), when three countries of the Global South – Brazil, Cuba, and Iran – proposed to create an intergovernmental framework to replace the existing ICANN-led internet governance model (Bhuiyan, 2014, p. 51). In essence, these countries demanded "their sovereign right to make international public policy for the internet" (Mueller, 2020, p. 3).

In the second preparatory committee of the WSIS in Geneva in 2003, the head of the Chinese delegation criticized the status of internet governance as "monopolized by one state and one corporation that neither facilitate further growth of the internet, nor fully embody the principle of equity and full representation" (Negro, 2020, p. 10). During the WSIS, China's spokesperson tried to raise understanding for its restrictive approach to freedom of speech, calling the international community to "fully respect the differences in social systems and cultural diversity" (China, 2003). A key cultural issue discussed in WSIS was the question of domain names in non-Roman alphabets (Associated Press, 2005; Baasanjav, 2014).

Finally, the WSIS debates produced three opposing parties: Brazil, China, Russia, India, Pakistan, Iran, and Cuba, which advocated for governmental control of the internet within the UN; the US, which wanted to keep the status quo; and the EU, which initially supported the demand for governmental control over the internet, but then switched sides.

In the end, the resulting Tunis Agenda of 2005 recognized the call for digital sovereignty: "Policy authority for Internet-related public policy issues is the sovereign right of states" (WSIS, 2005). However, this declaration was

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

not followed by real changes since the US put high diplomatic pressure on the EU to withdraw its support for the proposal to replace ICANN with a system of intergovernmental control over the global internet ("Letter by Gutierrez and Rice," 2005). An observer summarizes: "The irony is even though Europe has been critical of ICANN, they have given their blessing to it" (Associated Press, 2005). With the European retreat, the countries favoring governmental control of the internet were relatively isolated. In the developed countries of the Global North (with the notable exception of France), the issue did not appear in the debate any more during these years (Benhamou & Sorbier, 2006; Thumfart, 2022).

Conversely, China and Russia furthered the agenda between each other and several former central Asian Soviet Union states within the SCO. Hereby, China is clearly the most important actor. In 2008, China surpassed the US in the number of internet users and has since been the leading country in terms of internet users (Robson, 2017). Accordingly, Beijing intensified its ambitions to strengthen national sovereignty over digital technology and promote this approach through international organizations such as the SCO and the BRICS.

In addition to the SCO, which will be dealt with in detail in Section 2.5, the ITU is an important forum, of which the secretary-general was Chinese from 2015 to 2022. Another important forum is the Beijing-initiated and -controlled World Internet Conference (WIC), which started in 2014 and included representatives of SCO member states, observers, and the private sector, for instance, companies and organizations such as Baidu, Alibaba, Tencent, Apple, Amazon, Microsoft, Samsung, LinkedIn, and ICANN. Since 2014, China has been promoting a declaration regarding digital sovereignty that was officially presented to the participants of this conference in 2015 (Zeng, 2015).

2.5 DIGITAL SOVEREIGNTY IN THE SCO SINCE 2005

The SCO was founded in 2001 based on a treaty regarding central Asian border conflicts in 1996 that gave birth to the "Shanghai Five." Its original members were China, Russia, Kyrgyzstan, Kazakhstan, Tajikistan, and Uzbekistan. At first, Russia was its driving force with the two-fold strategic objective to prevent Western interventions following the wars in former Yugoslavia (1991–2001) and the "color revolutions" (2000–2005) as well as to combat Islamist extremism in the region that became a security threat with the conflicts in Chechnya and Dagestan and numerous terrorist attacks in the region (Souleimanov & Horák, 2006). The SCO's strategic goal against Western intervention and Islamic extremism connects cultural issues with security ones.

With a rising profile, China increasingly held more sway in the SCO. On issues concerning Xinjiang province, China shared the objective to combat Islamic separatists. The formation of the Regional Anti-Terrorist Structure

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

(RATS) in 2004 is the central pillar of the SCO and will be discussed later. In the context of its other objective, which is to strengthen state sovereignty against perceived Western interventions on issues such as human rights or popular consent, the SCO also served as a transmission belt for the Chinese imaginary of digital sovereignty to be exported to other member states. This applies foremost to Russia, which was concerned with Western interference but pursued a largely liberal approach to internet regulation until the Duma election protests of 2011 (see Section 2.6).

In 2005, the year of the Tunis Agenda of the WSIS, the SCO started to advance its strategic goals in digital sovereignty that bear resemblance to the NWICO or WSIS debates. The Astana Declaration of that year reads: "The world's diversity of cultures and civilizations is a universal human value. In an era of rapid development of information technologies and communications (…), the right of every nation to its own way of development should be fully guaranteed" (SCO, 2005).

The SCO's explicit demands for digital sovereignty fit well into this framework. These demands started with the *Declaration of the Heads of the SCO Member States on International Information Security* in 2006 that emphasized the willingness of the participants to collaborate. Although this declaration was explicitly following a recommendation included in the Resolution 60/45 passed at the 60th UN General Assembly on strengthening multilateral cooperation in matters of information security, it stands in evident contrast to the UN doctrine: The SCO member states emphasized a territorial understanding of sovereignty directly opposed to the global free flow of information. The signing member states stressed the need for international collaboration due to "the cross-border nature of ICT" but characterized ICTs as possibly contradicting the principles of "non-interference in the internal affairs of sovereign states" and "non-use of force" (SCO, 2006). Furthermore, the cultural aspect was explicitly stated in the SCO's 2006 declaration, particularly the "respect for religious feelings and traditions of nations, inter alia, within the Shanghai Cooperation Organization region."

Despite this rhetorical focus on territorial sovereignty, the SCO includes a significant degree of transnational cooperation in the service of preserving regime stability. In this sense, the SCO has been accurately labeled as "transnational authoritarianism" and criticized for being "a vehicle for human rights violations" (Tsourapas, 2020, p. 20). The SCO is built on the principle of mutual recognition within the Regional Anti-Terrorist Structure (RATS), which, for example, allows for the seamless extradition of individuals suspected of terrorism and the exchange of relevant information (International Federation for Human Rights, 2012, p. 5). In the language of the SCO, this is part of fighting the "three evils" of terrorism, separatism, and extremism. However, from a Western perspective, this constitutes transnational repression against individuals who can be regarded as dissidents, such as several Uyghur activists (International Federation for Human Rights, 2012, p. 16).

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

The SCO's Agreement on Cooperation in Ensuring International Information Security of 2009 was likewise a reaction to a UN resolution on multilateral cooperation in the field of information security. Outspoken about its fears of regime change orchestrated by the West, the agreement names what it considered "major threats in the field of international information security" including not only "information warfare," "information terrorism," cybercrime, but also the "use of a dominant position in the information space to the detriment of the interests and security of other states" and "dissemination of information prejudicial to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other states" (SCO, 2009).

The Tashkent Declaration of 2010 clearly formulated the SCO project to create a normative order of cyberspace based on territorial sovereignty:

> Information security is closely linked to state sovereignty, national security, socio-economic stability and the interests of citizens. All countries are entitled to exercise control over the Internet in accordance with their domestic situation and laws, while expanding cooperation in a spirit of equality and mutual respect (SCO, 2010).

In 2011, the SCO member states submitted a Draft International Code of Conduct for Information Security to the UN General Assembly very much in line with China's position at the WSIS. The draft reaffirms that "policy authority for Internet-related public issues is the sovereign right of states" (McKune, 2011). The text also includes a condemnation of cyberwar. The drafters pledge "not to use information and communication technologies, including networks, to carry out hostile activities or acts of aggression." Furthermore, it includes a passage that, once more, directly links cultural issues to security issues, in which the drafters agree to combat the "use of information and communications technologies (…) that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment." Little was changed in a new draft submitted to the UN General Assembly in 2015.

It is difficult to assess the impact of the SCO's rhetorical positions on existing policies. None of the regimes involved is particularly transparent, especially when it comes to security issues. In terms of the digital implications of the SCO, it is certain that the Regional Anti-Terrorist Structure (RATS) exists and that the SCO includes a regime of transborder exchange of e-evidence. But it is also likely that this organization is, in many aspects, a paper tiger. However, at the international level in particular where norms tend to be contested and permanently evolving, rhetoric can be extremely influential in the construction of sociotechnical imaginaries. In this sense, the declarations analyzed in this section demonstrate that the SCO served as a transmission belt for a sociotechnical imaginary of digital sovereignty that connects cultural issues with security issues in the digital realm.

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

2.6 DIGITAL SOVEREIGNTY IN RUSSIA SINCE 2011

Although the Soviet Union played a leading role in the NWICO debates and even criticized the NWICO for *not being focused enough* on sovereignty, the post-Soviet discourse on domestic sovereignty and digital technologies is not as elaborate as the Chinese discourse on this matter (MacBride & Commissioners, 1980, p. 280). An indicator for this is that Cyrillic domain names did not get introduced before 2010 (Radio Liberty Staff, 2010), while Chinese domain names were introduced independently from ICANN as early as 2000 (Arséne, 2015, p. 30; Baasanjav, 2014, p. 966). For a long time, Moscow even promoted a moderate form of freedom of speech on the internet since it regarded the digital public sphere as a "social decompression chamber" that would keep people out of real politics (Nocetti, 2017). Rather than censoring, the Russian government initially supported the development of a regime-friendly digital sphere including bloggers, influencers and institutions that would later become notorious as Russia's "troll factories" (Morozov, 2011, p. 126).

For this reason, China seems to have played the leading role in the propagation of more restrictive digital policies in the context of the SCO's early declarations. Around the year 2016 when the Chinese promotion of this matter within the ITU, SCO, and WIC reached a peak, Russia reportedly received surveillance and censorship technology from China (Soldatov & Borogan, 2016). Some suggested already earlier that Russia has been demoted from the leading force of the SCO to China's "junior partner" (Aris, 2008, p. 14).

However, the Chinese and Russian positions regarding digital sovereignty are complementary within the SCO and the BRICS contexts. While the Chinese discourse was from the start more focused on defensive sovereignty, the Russian one was more focused on aggressive digital sovereignty (Soldatov & Borogan, 2018). The first Russian (then still Soviet) cyberattack on the US happened as early as 1986 (Stoll, 1989). In 2007, the Kremlin's youth organization Nashi's attack on Estonia marked the beginning of the contemporary cyberwar discourse in the West by triggering the instalment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.

Then again, both China and Russia are subject to similar external drivers since they are geopolitically opposed to the cyber-hegemon USA and its actions, which became globally notorious with the Snowden revelations of 2013. The notion of "Суверенный интернет" ("Sovereign Internet") finds its origin in a column published some weeks after the Snowden revelations of 2013 by Sergei Zheleznyak, a leading politician for implementing Putin's authoritarian turn (Elder, 2013). Under the umbrella of digital sovereignty, Zheleznyak condemned the US, demanding a "national server network" and Russia's "own information products." Subsequently, in 2013, the *Internet Research Agency* was founded, which later influenced the US's 2016 election in an "attempt to duplicate what the Kremlin considered the West's unwarranted incursions into Russia's own political life" (Krastev & Holmes, 2019, p. 118). Furthermore, in 2016, the Yarovaya Laws on data localization have been passed, which require personal data from individuals located in Russia to be stored within Russian territory (Savelyev, 2016). Russia also pursued an infrastructural sovereignization of RuNet (Sivetc, 2021).

These measures of sovereignization are also the product of an earlier turning point than the Snowden revelations in 2013. In 2011, following the Arab Spring, Russia experienced the greatest wave of protests of its post-Soviet history, many organized through the internet (Asmolov, 2020, p. 243). Moscow believed these protests to have been orchestrated by the US (Snyder, 2018b), even though the main reasons for these protests were, in fact, domestic (Robertson, 2013). As a reaction, Moscow started to tighten political control of the internet (Harper, 2017), passing a "whole avalanche of new repressive laws" (Weiss, 2016, p. 289). In 2012, the state introduced Federal Law 139 FZ, which, at first, banned sites containing child pornography, information regarding suicide, and selling drugs, which would two years later, with the Law 398 FZ, also extend to political content (see Chapter 8). This form of internet censorship is, at least, rhetorically, closely related to cultural issues. The repressive laws crucial to internet censorship, all adopted around the year 2012, target blasphemy, obscene language and "propaganda of non-traditional sexual relations."

It is noteworthy that the cultural/religious turn marked by these laws was well understood in Russia, particularly the anti-blasphemy laws that triggered protest by the traditionally secular communists (Weiss, 2016, p. 290). In turn, the laws against obscene language produced less resistance and were accepted as a continuation of a Soviet tradition. However, here too a shift was visible. While the prohibition of obscenities in Soviet times was connected to insults and offenses, the new laws "are exclusively aimed at establishing and promoting language norms" (Kovalev, 2016, p. 339). The case of the so-called antigay laws is even more complex since they are based on irrational ideas. At least rhetorically, Moscow regards communication regarding homosexuality as part of Western information warfare with the objective to reduce low Russian birth rates even further (Mortensen, 2016, pp. 353–357). Overall, these concepts and laws are vague and it is exactly their vagueness and irrational nature that allows for the most repressive interpretations (Weiss, 2016, p. 289).

Some of the most notorious examples of these laws include investigations against a blogger who posed as a priest on Instagram and the forced psychiatric admission of a user of VKontakte who denied the existence of God (Weiss, 2016, p. 290). Another prominent example is the manager of a feminist website who was trialed for pornography and gay propaganda and put under house arrest (Amnesty International, 2019). Russia's internet laws have a strong chilling effect on civil society beyond these individual cases.

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

While it is relatively easy to connect the Chinese discourse on digital sovereignty to cultural and political specifics such as Confucianism and Marxism, this is much harder in the Russian case. As mentioned before, the incompatibility of the Cyrillic and the Roman alphabet plays a role in the Russian pursuit of digital sovereignty, and so does Moscow's involvement in conflicts with Islamist extremism in Chechnya and Dagestan.

However, the cultural conflict with Islamist extremism unfolds very differently in Russia since Moscow and the Orthodox church are sympathetic to the illiberal cultural claims of Islamism. For example, in contrast to Western European countries, the Russian government has banned Charlie Hebdo's satirical depictions of Mohammed for "inciting religious hatred" and the Orthodox church supported this step (Rainsford, 2015). On a number of occasions, Putin read from Quran, Bible, and Talmud at the same event, which expresses a close linkage between politics and religion (Black, 2021, p. 377).

These are examples of the inclusive, yet illiberal, imaginary of Русский мир (*russkii mir*) that undergirds Russian politics on many levels. The term "*russkii mir*" can be understood as "Russian World," which includes the canonic territory of the Orthodox Patriarchate, that is, Ukraine, Belarus, Moldova, Kazakhstan, and many other Slavic countries. The term can be also understood as "Russian Peace" in a sense of *Pax Russica* that constructs the notion of Russia's hegemony (Laruelle, 2015, p. 15) over a multicultural Eurasian space corresponding to the idea of Russia as a "Third Rome" (Poe, 2001). In addition to these rather conservative and expansive connotations, the idea of the "Russian World" includes the territory of the former Soviet Union.

Despite its baroque multiplicity of historical fields of resonance, this idea of the "Russian World" is extremely relevant politically. On March 18, 2014, Putin used it as a justification for Russia's annexation of Crimea (Laruelle, 2015, p. 15). Typical of imperial imaginaries, the lack of geographical precision makes the concept of the "Russian World" useful for the justification of any kind of territorial expansion.

The ultranationalist Russian think tank *Izborsk Club* close to Putin formulated a Russian messianic mission for Eurasia on these grounds, which includes combatting the cultural effects of informational globalization. Its manifesto from 2012 reads:

> The lethal ideological and informational "machine" that destroyed all the bases and values of the (…) Romanov empire and then destroyed all the foundations of the (…) Soviet empire is everywhere at work. The fall of these empires transformed the great Eurasian space into a chaos of warring peoples, faiths and cultures on fields of blood. (…) The Russian messianic consciousness, grounded (…) in the Orthodox dream of divine justice (…) summons the negation of Russia at the level of worldview, the attacks on her faith, culture, and historical codes (Snyder, 2018a, pp. 93–96).

From the point of view of the intellectual history of sovereignty, an interesting feature is Russian leadership's reference to German authoritarian legal theorist

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

Carl Schmitt's realist conception of international relations, which is widely shared among Eurasia ideologues (Snyder, 2018a, pp. 80–90). Schmitt's arguments against the illegality of wars of aggression partially explain Moscow's "hybrid warfare" of kinetic and cyber means (Renz & Smith, 2016; Snyder, 2018a, pp. 193–194). Of course, Moscow's stance is characterized by double standards. While promoting noninterference in the digital sector on a normative level, for example, within the SCO and the BRICS, it engages in using kinetic and cyber means for projecting power.

Schmitt's idea of sovereignty, namely its foundation in the state's monopoly of force and control and its emphasis on territoriality, is also a crucial feature of the Russian discourse on digital sovereignty. The "sovereign internet" (Суверенный интернет) grants the government far-reaching control, including deep-packet inspection of transnational data traffic. In 2019, Russia reportedly disconnected its internet from the global one, without ordinary citizens noticing it (Wakefield, 2019). Leonid Savin, a Eurasia political activist of the *Izborsk Club*, points out that sovereignty in the territorial Schmittian sense requires a realignment of cyberspace with territory, which must ultimately include the possibility to disconnect at will from global communication (Savin, 2019a, 2019b).

However, it should be noted that the Russian government's decidedly illiberal approach to digital sovereignty has its technological limits. For instance, Moscow's unsuccessful attempt to ban Telegram has shown that there is a merely rhetorical element to its claims of digital sovereignty (see Chapter 8). As of mid 2024, the jury is still out as to how the Russian army may perform on the kinetic battlefield and the cyber domain. So far, Moscow has not yet attempted the actual "disconnect" of RuNet from the global internet. However, it must be stressed that rhetoric matters when it comes to international norms and the construction of sociotechnical imaginaries.

2.7 DIGITAL SOVEREIGNTY IN INDIA SINCE 2017

India is the most complex of these three nations in terms of digital sovereignty formations. While India was a driving force behind the BRICS from the start with the creation of the BRIC in 2006, it is connected to the SCO in a loose way since it joined the SCO only in 2017. India was invited by Russia to join the SCO to counter China's invitation of India's archrival Pakistan. It is unclear to which extent previous declarations of the SCO will concern India as the country is a "digital decider" between liberal and non-liberal modes of digital governance (Basu, 2019). For instance, India joined the majority of the SCO and BRICS member states in backing the adoption of the UN resolution on *Countering the Use of Information and Communication Technologies for Criminal Purposes* (Sherman & Morgus, 2018).

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

India has a strong bipartisan anti-colonial tradition, which includes a general willingness to defend local cultures and economy against global hegemonic structures. Actors closer to the politically left promote a form of economic nationalism called *swadeshi* ("swa" = "self" and "desh" = "country"), while actors on the politically right promote *hindutva* ("Hindu-ness") (Prabhu, 2012). India has also been one of the leading forces of the Non-Aligned Movement, which was crucial to the NWICO debate in the 1970s and 1980s. During WSIS, too, India has been on the side of those nations who demanded more political oversight over internet governance (Vipin, 2011).

Comparable to China, the resistance against US-led digital colonialism is important to India, where a commentator labeled Google's crushing of the country's local search engines as "digital battle of Plassey" (Arya, 2020). Accordingly, India has implemented a relatively strict regime of data localization that is primarily focused on the idea that the data of Indian citizens (the second largest internet user base in the world) constitutes an economic resource that should belong exclusively to Indians. This perspective focused on the national economy is particularly convincing since the country maintains the world's largest digital biometrical ID program Aadhaar, which has been installed as early as 2009. This technological-demographical baseline situation also brought about a focus on privacy and national security (Kovacs & Ranganathan, 2019, p. 17).

However, the country's position is characterized by a double frontline. In addition to a guarded stance against Western digital hegemony, India seems to also fear the influence of China, with whom it forged an alliance through the BRIC grouping since 2006 and through the SCO since 2017. India and China also had a number of territorial disputes beyond the digital realm, for instance, the 2020–2021 border skirmishes. The ban of dozens of Chinese apps in June 2020 that resulted from these border conflicts also made clear that India's digital sovereignty can be in direct opposition to China from time to time (Al Jazeera, 2021). Due to diverging and converging interests on different issues and at different times, the SCO and the BRICS grouping can experience instability given their multipolarity.

Culturally, the notion of *hindutva* embodies a nationalist aspect that became increasingly important to Modi's Hindu nationalist government (Mohammed-Arif et al., 2020). However, today, the focus of this ideology lies not so much in its stance toward the West, with whom the Modi government maintains tight relations, but toward Pakistan and the approximately 200 million Indian Muslims (Tellis, 2018). Furthermore, in contrast to Russia and China and although Modi's government promotes the replacement of English by Hindi on all levels of Indian society, global Anglo-Saxon culture may not be regarded as an existential threat from an Indian point of view as a significant part of its population speaks English as a second language. Neither does India have only one non-Roman alphabet, which would produce a clear dichotomy. Since 2011,

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

ICANN has allowed for domain names in several regional languages: Hindi, Gujarati, Urdu, Punjabi, Bengali, and Telegu (Sengupta, 2011). Compared to China, the liberal Western idea of internet freedom poses no fundamental ideological problems to India since the country is constitutionally a democracy.

However, comparable to the domestic implications of the Russian and Chinese imaginaries of digital sovereignty, internet use in India can also be heavily restricted. This is largely owed to domestic security challenges related to religious issues. Already in the 2000s, the Indian government has shown a keen interest in cybersecurity due to Islamist terrorism (Kovacs, 2021, p. 134). Modi's Hindu nationalist government, in turn, stoked interreligious conflicts (Mohammed-Arif et al., 2020). In India's complex society full of inner tensions and anachronisms, such conflicts and conflicts of nonreligious nature can lead to violent online mobs, often fueled by disinformation. In August and September 2013, social media played a decisive role in stoking clashes between Muslims and Hindus in the state of Uttar Pradesh, which left 62 dead, 93 injured, and 50,000 displaced (Biju, 2019, p. 10). Also, following the anti-Muslim laws issued by the Hindu Nationalist government, the Delhi riots of 2020 killed 53. The riots were clearly of interreligious nature, stoked by hate spread through social media (Mehta, 2020). In another example from 2018, two young men were accused of being child kidnappers and were beaten to death on the grounds of a social media video (Deutsche Welle, 2018). Such lethal attacks on the basis of social media rumors occurred more frequently in India (Krishnan, 2018). In the first half of 2018 alone, more than two dozen people died related to rumors spread via WhatsApp (Samuels, 2020). In many cases, the perpetrators were "rightwing Hindu cow vigilantes" (Shah, 2021, p. 1932). However, in one of the latest such incidents – the 2020 Palghar mob lynching – two men were killed on the grounds of WhatsApp rumors, and both the perpetrators and the victims were Hindu.

Such incidents, which the Hindu nationalist government partly stoked, serve as the justification for the government's more expansive control over web content. For instance, the Indian government has requested Twitter (now X), Google, and YouTube to remove posts considered blasphemous or inciting communal violence (Segal, 2017). In 2019, Netflix agreed to delete all content that disrespects the country's flag, hurts religious sentiments, or promotes terrorism (Dixit, 2019). After the Indian government waged a "war with Twitter" (Biswas, 2021), Twitter too agreed to delete 90–95% of accounts requested for removal by the Indian government (Business Insider India, 2021). However, since the removal requests concerned mostly the accounts of anti-government protesters, it is obvious that the Indian state's actions do not exclusively serve security purposes, but also the government's own interest.

Since the Temporary Suspension of Telecom Services Rules came into force in 2017, the Indian government also frequently uses these rules to enact local "internet shutdowns." Although this practice also exists in Western democracies (De Gregorio & Stremlau, 2020), India is, by far, the number one country

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

in enacting such shutdowns. Of the 155 internet shutdowns imposed globally in 2020, a staggering 109 occurred in India, which means that the country is even more authoritarian on this issue than other SCO member states (Chakravarti, 2021).

India has also enacted one of the world's longest and most far-reaching internet shutdown so far, lasting from August 4th, 2019 to March 4th, 2020 affecting the former Muslim-majority state of Jammu and Kashmir with 12.5 million inhabitants (Internet shutdowns in India, n.d.). The toll on the local economy and on civil society, particularly the work of journalists, is high (Sarkar et al., 2020). An analysis from 2019 has shown that shutdown orders mostly do not require suspension of internet services in their entirety, but rather a direct blocking of specific mass messaging platforms such as Facebook, Twitter, and WhatsApp (Internet Freedom Foundation, 2019). Furthermore, internet shutdowns became so common in India that they are not always seen as political or security issues. In widely criticized displays of local authoritarianism, local governments regularly suspend internet connectivity to ensure that no cheating takes place during civil service exams (Sanzgiri, 2023). This is to be understood not only as a display of authoritarianism but also as an expression of the "heavy emphasis on education in the country, where for many, proper schooling could be the key out of poverty" (Yeung et al., 2021).

Also beyond the measures mentioned earlier, the current Hindu nationalist government promoted digital authoritarianism (Sherman, 2019). It has extended the use of artificial intelligence-enabled facial recognition in urban centers and successively transformed the country's digital biometrical ID program Aadhaar from a voluntary to a de facto compulsory ID since it is needed for a great number of governmental services. This, too, has been raising fears of governmental surveillance (Khera, 2019). This top-down authoritarian turn is worsened by increasing digital vigilantism in the Indian civil society of the so-called "cyber Hindus" (Biju, 2019, p. 10).

In summary, the Indian concept of digital sovereignty includes highly authoritarian aspects, most notably censorship and internet shutdowns, which are partly connected to complex authoritarian strategies of the Hindu nationalist government but the concept has also to be understood within India's complex cultural contexts. While the Russian notion of a disconnectable "sovereign" internet explicitly refers to Schmitt's understanding of sovereignty against foreign powers, the Indian concept of digital sovereignty realizes the Schmittian principle on the domestic level as Schmitt defined sovereignty as the power to declare the state of exception, and internet shutdowns are an expression of such a "liminal" understanding of sovereignty in the digital realm (Thumfart, 2024a).

It is important to note here that such dramatic authoritarian approaches include a great degree of make-belief. It is more than questionable whether internet shutdowns actually achieve their security goals since they have been found to be combined with governmental inaction in critical situations of civil

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

unrest (Ruijgrok, 2021, p. 32). Furthermore, it is not possible to shut down the internet in a country completely (Shah, 2021, p. 2696). However, there is no doubt that internet shutdowns represent an impressive staging of the nation-state as "taking back control" over digital networks. And such staging of governmental power matters, particularly regarding sociotechnical imaginaries.

2.8 CONCLUSION: DIGITAL SOVEREIGNTY FOR GLOBAL CULTURAL DIVERSITY?

Digital communication has become a decisive factor in the economy and politics of all countries. A critical understanding of the global digital infrastructure and economy as enabling "digital colonialism" is not entirely unjustified even for authoritarian countries (Avila Pinto, 2018; Hicks, 2019). Neither are fears that democratization campaigns based on social media might lead to regime change – regardless of whether this regime change might be desirable from a human rights perspective or not. Developing nations with non-liberal traits, as in the cases of China, Russia, and India, have constructed imaginaries of digital sovereignty that can be evoked to implement economic protectionism and political censorship. Such obstacles to the domestic and transnational free flow of information often include violations of article 19 of the UDHR.

Beyond political and economic aspects that influence the imaginaries of digital sovereignty promoted within the SCO and the BRICS by China, Russia, and India, it is crucial to consider cultural factors. Although threats to national cultural identities are often exaggerated and politically exploited, governments and civil societies of all three nations do have reason to believe that their traditional culture can be threatened by the free flow of information enabled by global digital hegemons. As a matter of simple fact, ICANN for a long time allowed only top-level domains in the Roman alphabet. Additionally, all of these immensely diverse countries hardly fit the idea of consolidated nation-states following the European pattern of development for they are often confronted with significant internal cultural conflicts. Whether perceived or real, internal cultural challenges and external cultural threats have informed these countries' non-liberal or authoritarian positions on domestic digital sovereignty in the form of censorship and on external digital sovereignty in the form of protectionist policies, and in the case of Russia, also aggressive cyber operations.

This chapter highlights the relationship between digital sovereignty and cultural identity. It does so by tracing the historical narrative that informed the development of the notion of "cultural sovereignty" during the NWICO debates in the 1970s and 1980s, the digital sovereignty discourse that emerged in China in the 1990s, and the subsequent spread of an extreme form of state-centric digital sovereignty to Russia since 2011 and the embrace of it by a nationalist Indian government from 2017 on. In these processes,

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

the multilateral forums of the SCO, and to a lesser extent the BRICS, served as a transmission belt in proliferating state-centric imaginaries of digital sovereignty. It is a central finding that in all three of the examined countries, imaginaries of digital sovereignty are related to a non-secular understanding of the state that merges politics and religion (Russia and India) and traditions that are neither secular nor religious (Chinese Confucianism). And since 2006, SCO statements routinely connected religious issues, information technologies, and security concerns. In this sense, the global emergence of digital sovereignty can be compared to the evolution of state sovereignty from the confessional wars and the connected development of the printing press in sixteenth- and seventeenth-century Europe. On a methodological level, this chapter demonstrates that, similar to this more or less well-fitting historical comparison, the construction of state-centric digital sovereignty can only be understood considering a complex entanglement of domestic social, economic, political, and cultural dispositions, power dynamics in international relations, and the development of concrete technological capacities (see also: Thumfart 2024b).

As of 2024, it is difficult to speak in positive terms of a common future of the BRICS or SCO that includes a militaristic Russia, as doing so may normalize Russia's aggressive authoritarianism that is not shared by China or India. However, a more hopeful long-term outlook for the BRICS beyond Russia's war of aggression in Ukraine and Putin's misrule could emphasize cooperation between BRICS nations to realize the objectives set by NWICO and WSIS by making the digital world less one-dimensional or monopolistic (see Chapter 1). One does not need to be a right-wing nationalist to regard global cultural assimilation as a problem. If one takes the impact of digital communication on the development of human civilizations seriously, then US-led standardization and destruction of cultural diversity by Googleization, Facebookization, Twitterization, and Uberization could constitute a threat to human civilizations severe enough to warrant a serious response. Due to prejudices incurred by biased algorithms and faulty AI, cultural diversity is more than a nice-to-have luxury, but of vital importance to adequately represent the full scope and complexity of human social and intellectual capacities. Digital sovereignty grounded in legitimate reasons and proportionate actions can be a crucial means to protect cultural diversity across the globe and harvest its potential.

If one assumes that regulation of digital content and services to preserve cultural diversity around the globe is legitimate, where does the legitimate interest in preserving one's own culture end and where does the persecution of religious and other minorities begin, as this is the case of Muslims, dissidents and members of the LGBTQ+-community in China, Russia, and India? What about respecting citizens' privacy and right to communicate freely across borders and conduct business online when doing so contradicts the interest of the state? These are difficult questions. Decolonization and authoritarianism

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press

converged historically in their shared resistance against Western norms, which are frequently thought of as including human rights such as the freedom of speech and the right to privacy (Watson, 2021). An informed debate on digital sovereignty has to consider both: the dangers of digital authoritarianism and the productive potential of digital decolonization.

Funding acknowledgement: During this research, Johannes Thumfart received funding from *Gerda Henkel Stiftung's special programme Security, Society, and the State* (2020–2022) *and the European Union Horizon 2020 research programme under MSCA COFUND grant agreement 101034352 with co-funding from the VUB-Industrial Research Fund* (2022–2024).

https://doi.org/10.1017/9781009531085.004 Published online by Cambridge University Press