INSTITUTO SUPERIOR
DE CIÊNCIAS SOCIAIS
E POLÍTICAS
UNIVERSIDADE DE LISBOA

Daxiyangguo
Portuguese Journal of Asian Studies | Revista Portuguesa de Estudos Asiáticos
ISSN: 1645-4677 | ISSN-e: 2184-9129 | 2024, 2.º semestre, Número 33, páginas 13-32
DOI: 10.57857/ulisboa.iscsp.1645-4677.33.2024.000002/pp.13-32

China's Role in Shaping the BRICS Agenda for Digital Sovereignty

O Papel da China na Definição da Agenda dos BRICS para a Soberania Digital

Inês Rito *

* Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa, Centro Científico e Cultural de Macau (CCCM), Portugal; Email: inesrito22@gmail.com

ABSTRACT
This paper analyzes how China's conception of digital sovereignty aligns with the BRICS agenda for global internet governance. The analysis discloses China's state-centric approach to cyberspace regulation and its efforts to promote this vision through diplomatic channels and strategic partnerships, primarily within the BRICS framework. The paper also broadly considers the varying perspectives on digital sovereignty held by other BRICS nations, highlighting the complex and uneven landscape of this issue within the group. While some countries, like Russia, closely align with China, others, such as India, seek to reduce dependency on Chinese technology. We argue that, while the BRICS countries have diverse perspectives on digital sovereignty and Chinese digital investments, China's position as the largest economy in the group

allows it to exert significant sway over the coalition's stance on the issues of non-interference and digital sovereignty.

Keywords: BRICS; China; digital sovereignty; cyberspace governance

RESUMO

O presente artigo analisa a forma como a conceção chinesa de soberania digital se alinha com a agenda dos BRICS para a governação global da Internet. A análise expõe abordagem chinesa à regulação do ciberespaço centrada no Estado e os seus esforços para promover esta visão através de canais diplomáticos e parcerias estratégicas, principalmente no âmbito dos BRICS. O artigo considera amplamente as diferentes perspetivas relativamente à soberania digital dos BRICS, destacando o panorama complexo e desigual desta questão dentro do grupo. Enquanto alguns países, como a Rússia, se alinham estreitamente com a China, outros, como a Índia, procuram reduzir a dependência da tecnologia chinesa. Argumenta-se que, embora os BRICS tenham perspetivas diversas sobre a soberania digital e sobre o investimento digital chinês, a posição da China como a maior economia do grupo permite-lhe exercer uma influência significativa sobre a posição da coligação relativamente às questões de não-interferência e de soberania digital.

Palavras-chave: BRICS; China; soberania digital; governação do ciberespaço

1. Introduction

Coined initially as “BRIC” by economist Jim O'Neill in 2001 to highlight the growing economic power of Brazil, Russia, India, and China, the alliance officially became known as BRICS in 2010 when South Africa joined. This broadened its geographical and economic representation, establishing itself as a significant coalition of emerging economies with substantial influence in global affairs. In 2023, the group expanded to include Saudi Arabia, Egypt, Ethiopia, Iran, and the United Arab Emirates (Cardoso, 2023). Together, they comprise 46 % of the global population and about 25 % of global GDP (O'Neill, 2024). As evidenced by the establishment of new financial institutions, namely the New Development Bank (NDB) and the Contingent Reserve Arrangement, these countries seek to reform global governance to improve the advocacy for the interests of developing countries (Mazenda & Ncwadi, 2016).

The interest in cybersecurity cooperation among BRICS countries was formally highlighted in the 2013 eThekwini Declaration and Action Plan, adopted after the fifth BRICS Summit. The timing of this declaration was particularly noteworthy, as it followed the high-profile revelations by Edward Snowden, which exposed widespread global surveillance activities by the

United States National Security Agency (NSA) (Jiang, 2021), which accentuated the urgent need for enhanced cybersecurity measures and international cooperation, prompting the BRICS countries to prioritize this issue in their strategic agenda (Belli, 2021).

Cyberspace is generally understood to encompass the digital realm, comprising various forms of digital communication such as the internet, telecommunications networks, computer systems, and embedded processors and controllers (NIST, 2011). In contemporary times, it has evolved into a contested political domain akin to other physical spaces like maritime, airspace, and outer space (Barrinha & Renard, 2017). In this field, cybersecurity issues are closely linked with political considerations and perceived state threats. Discussions about cybersecurity policy and internet governance involve topics such as political censorship, unfair competition, and assaults on critical infrastructure (Lindsay, 2015).

Drawing from the traditional concept of sovereignty, digital sovereignty can be perceived as "(...) independence of a state in the digital sphere and its ability to implement the information policy of its own choice domestically and internationally. Digital sovereignty currently entails control over the communications and Internet infrastructure within the state borders, independence both in software and platform economics, which implies the presence of national search engines, social network services, postal services, etc. in a given country" (Ignatov & Zinovieva, 2024, p. 3). As a concept, digital sovereignty is regarded in numerous ways by literature. While the state-centric perspective is commonly discussed, authors such as Belli and Jiang (2024) propose a conceptual mapping where digital sovereignty can be exercised by multiple actors within the context of BRICS. This outlook englobes perspectives like supranational digital sovereignty and corporate digital sovereignty (Belli & Jiang, 2024). China holds a state-centric perspective of digital sovereignty, where the regulation of cyberspace by the state and non-interference policy is enforced (Wang, 2020). To get a better understanding of the Chinese approach, it becomes imperative to delve into the evolution of Chinese Internet governance and how digital sovereignty becomes the basis of the country's policy for cyberspace.

Following a phase of bolstering relations and integrating into the international order, conditions were ripe for China to extend its global positioning and exert influence over global governance. Central to the strategy is the enhancement of partnerships with both regional and international organizations, as well as securing markets vital for economic development. The construction of a robust global network of partnerships was imperative,

encompassing collaborations such as the BRICS, G20, and the Shanghai Cooperation Organization (SCO) (Cooper, 2020). The Belt and Road Initiative (BRI) also stands as a clear illustration of the country's intricate engagement in foreign affairs. It relies on a multitude of stakeholders, including financial institutions like the Asian Infrastructure Investment Bank (AIIB) and the China Development Bank, alongside local governments and several others, thereby introducing a new approach to policymaking, which showcases the determination to contest Western-dominated global norms and institutions (Brown, 2020). China has also been at the forefront of advancing digital transformation and fostering economic cooperation within the BRICS bloc through several ICT initiatives demonstrating its commitment to driving technological innovation within the group (Chinese Academy of Cyberspace Studies, 2023).

The BRICS framework facilitates collaboration across various domains, allowing member countries to address shared challenges and pursue common goals. One of the critical debates within this framework, particularly relevant to the concept of digital sovereignty, centers on the divergent perspectives regarding the role of major countries in the Global South (Fischer, 2022). On the one hand, scholars argue that these nations seek to challenge and reshape the existing global order to better align with their interests and aspirations. On the other hand, there's a contrasting viewpoint that these countries, despite their grievances, may prefer to operate within the current system from which they derive significant benefits, thus exhibiting a reluctance to fundamentally transform it (Moraes, 2020).

The primary objective of this paper is to examine the alignment of the Chinese concept of digital sovereignty with the BRICS agenda for global internet governance. The paper argues that China's robust economic and diplomatic standing affords it substantial influence within the group, regardless of prevailing political and economic divisions. The analysis will explore China's ambitions for digital sovereignty and its strategy for governing cyberspace within the framework of its foreign policy. Additionally, the paper will provide an overview of BRICS cooperation, encompassing BRICS initiatives on ICT development and China's digital footprint in the designated countries. Furthermore, it will delve into the individual perspectives of Brazil, Russia, India, and South Africa on digital sovereignty.

2. China's approach to digital sovereignty

China's advancement in the field of information and communication technology (ICT) started in the 1990s with a notable period of informatization.

During this phase, the Chinese government emphasized the growth and enhancement of ICT capabilities, establishing the groundwork for the country's contemporary digital infrastructure. This era saw substantial investments in telecommunications, the establishment of the Internet, and the proliferation of digital technologies across various sectors. The aim was to integrate ICT into the broader economy and society, thus fostering a digital transformation that could support China's rapid economic growth and modernization efforts (Hanna & Qiang, 2010).

In the 2000s, China entered a period of securitization to address the challenges and vulnerabilities that arose from its rapid ICT development. This phase focused on enhancing the security and resilience of China's cyberspace. The government implemented stricter regulations, established cybersecurity frameworks, and promoted the development of domestic technologies to reduce reliance on foreign entities. This shift was driven by the need to safeguard national security, protect critical infrastructure, and ensure the integrity of information systems in the face of growing cyber threats and international competition (Lee, 2022).

Currently, China is experiencing a stage of increased self-sufficiency, particularly in the tech sector. This contemporary period is characterized by a strong emphasis on developing indigenous technologies and reducing dependency on foreign technology and know-how (Creemers, 2020). The Chinese government has launched several initiatives to support homegrown innovation, such as the Made in China 2025 plan and the China Standards 2035, as well as significant investments in research and development (Koty, 2020). These efforts are designed to build a robust domestic tech industry that can compete globally, secure China’s technological future, and maintain its sovereignty (Belli, 2021). The Great Firewall of China, officially known as the Golden Shield Project, represents a pivotal component of China's strategy to assert digital sovereignty and control over its internet landscape (Griffiths, 2019), comprising a system of internet censorship and surveillance that restricts access to foreign websites, blocks internet tools, such as Google, Facebook, Twitter, and VPNs, and monitors online activities within the country. The Great Firewall uses several technological methods such as IP blocking, Domain Name System (DNS) filtering and redirection, URL filtering, and packet inspection, which restrict the flow of information that the government considers politically sensitive or harmful to national security, maintaining strict control over the online environment (Quan, 2022).

China's cyberspace governance framework involves key institutional actors like the Central Cyberspace Affairs Commission (CCAC), chaired by

Xi Jinping, overseeing the entire cyberspace system and the Cyberspace Administration of China (CAC), which works as a supporting organ to the CCAC. Other essential actors involved in cyberspace governance include the Ministry for Industry and Information Technology (MIIT), the China Academy for Information and Communication Technologies (CAICT), the National Information Security Standardization Technical Committee (TC260), the Ministry of Public Security (MPS), the Ministry of State Security (MSS), the Ministry of Foreign Affairs (MFA), and the People's Liberation Army (PLA) (Lee, 2022).

China's strategy for cyber sovereignty involves centralizing cyber policy decision-making under the oversight of the CAC, which reports to the CCAC. This approach includes drafting cyber laws and policies to address internal needs and respond to external trends, with the Cybersecurity Law (CL) serving as the foundation of China's cybersecurity policymaking. Moreover, China has made institutional, legislative, and developmental adjustments to enhance technological capacities and cybersecurity oversight (Jiang, 2021).

Considering the legal framework, the CL sets regulations for data localization and the transfer of data across borders (Jelinek, 2023). Moreover, the Personal Information Protection Law (PIPL), also known as the Chinese Data Protection Law, provides comprehensive rules for the processing of personal and sensitive information by specifying the legal basis for data processing, disclosure requirements, and the rights of data subjects. It also outlines strict requirements for international data transfers to third parties, ensuring that data leaving China's borders is adequately protected (PIPL, 2021).

In the context of Chinese foreign policy, the government employs the term 'core interests' to refer to the nation's best interests. These interests are officially defined to encompass state sovereignty, national security, territorial integrity and national reunification, the political system established by the Constitution, social stability, and basic protection to ensure sustainable economic and social development (China State Council, 2011). Regarding cyber matters, Chinese foreign policy endeavors to achieve the same objectives described in the 2022 White Paper titled "Jointly Building a Community with a Shared Future in Cyberspace" (China State Council, 2022). The primary goals are to respect digital sovereignty, protect digital peace and security, encourage openness and cooperation, and maintain digital order.

According to Broeders & Berg (2020), cyber sovereignty is the fundamental principle that guides China's approach to interstate relations in cyberspace, which is characterized by an emphasis on domestic information governance

and the core principles of non-interference and self-determination. Under this framework, China prioritizes the autonomy of states to manage their cyberspace and refrain from external interference while advocating the right of nations to independently determine their digital policies. The Chinese conception of sovereignty is rooted in the objective of upholding their political structure, safeguarding the integrity of China's governance system, and defending against external influences that may challenge it (Creemers, 2020).

As Benson e Zeng (2018) argue:

> China has made increased efforts to promote the concept of 'Internet sovereignty' as an alternative to the existing cyber norms. Contrary to the US/Western position that cyber space is an 'open' global commons beyond the sovereignty of any state, China's Internet sovereignty points to a more traditional state-centric, sovereignty-oriented regime (p. 10).

China is actively engaged in multiple international forums to advocate for the concept of digital sovereignty. Through participation in organizations such as the United Nations, the Shanghai Cooperation Organization (SCO), and the World Internet Conference (WIC), which is hosted in Wuzhen, China advocates for a model of internet governance that aligns with its national policies (Segal, 2017). This stance is also reinforced through regional organizations such as ASEAN, where China collaborates with member states to develop regional cybersecurity standards and protocols that align with its digital sovereignty principles (Gong, 2019).

3. Digital sovereignty in Russia, India, Brazil, and South Africa

The BRICS nations exhibit mixed approaches to digital sovereignty, reflecting their unique political, economic, and strategic contexts. In a similar fashion to China, Russia and India have implemented comprehensive strategies with the goal of minimizing reliance on foreign technology, specifically that originating from the United States. These countries prioritize self-sufficiency and the control of information within their borders. Russia and China, for instance, have implemented extensive measures to create indigenous technological ecosystems and robust cybersecurity frameworks, aiming to safeguard their digital infrastructures from external influence. India, similarly, has focused on promoting local technological industries and developing its digital solutions to enhance national security and economic independence (Belli & Jiang, 2024).

The Russian Internet landscape, referred to as RuNet, has become increasingly state-centered over the years. A significant development occurred

in 2016 when the Russian government hosted the "Internet+ Sovereignty Forum". During this event, the notion of establishing Russian standards and creating a more closed internet system was proposed (Ermoshina & Musiani, 2017). This trajectory culminated in 2019 with the passage of the "Sovereign Internet Law", a legislation that significantly expanded the government's ability to monitor internet activity and facilitated the creation of a national DNS. By allowing the government to control internet routing and access within the country, this law has further isolated the country from the global internet, enhancing state control (Stadnik, 2019).

India is committed to containing anti-government content (Ignatov & Zinovieva, 2024). Post-Snowden, India's Digital Public Infrastructure has significantly modernized governance and enhanced the country's digital sovereignty (Belli & Jiang, 2024). A critical development in this area is the creation of the Unified Payments Interface (UPI), a system that has revolutionized the financial sector by facilitating instant digital transactions, thereby reducing reliance on foreign financial systems and promoting greater economic independence (MC & Shanmugam, 2023).

Brazil presents a different stance, characterized by progressive and fluctuating policies. Initially, the country embraced Free Software policies to reduce dependency on proprietary software and gain greater control over its digital infrastructure. However, these policies have seen reversals, reflecting an inconsistent commitment to digital independence and technology control (Belli & Jiang, 2024). A significant step in Brazil's approach was implementing the "Marco Civil da Internet" (CGI.BR, 2014). This legal framework established principles for Internet usage and strong protections for personal data, aiming to ensure the rights of Internet users (Rezende & Lima, 2015). In response to the revelations by Snowden, one notable initiative is the construction of an ELLALINK undersea cable connecting Brazil to Portugal, designed to reduce reliance on US infrastructure for international data traffic (Blanc & Poznanski, 2018).

South Africa considers achieving digital sovereignty as linked to autonomy, legislative enforcement, and cybersecurity (Belli & Jiang, 2024). The country is primarily focused on infrastructure development and ensuring broad access to technology, rather than heavily regulating online activity (Ignatov & Zinovieva, 2024). A significant concern is managing the dominance of Big Tech companies (Ayodele, 2022).

4. BRICS cooperation overview

BRICS cooperation holds significant potential for mutual benefits and enhanced governance. Besides the joint initiatives on ICT development, an exemplary achievement is the creation of the NDB, which has bolstered economic growth and increased trade among countries in the Global South (Duggan, Hooijmaaijers, Rewizorski, & Arapova, 2021). However, several challenges complicate this cooperation. The differences in regime types and power asymmetries among BRICS countries present significant obstacles (Moraes, 2020). Each nation has its own set of priorities, tensions, and internal challenges, which can hinder effective collaboration. For instance, the varying political systems and levels of economic development can lead to divergent policy approaches and strategic interests. Moreover, geopolitical tensions both within the group and with external powers can strain relations and inhibit unified action (Duggan, Hooijmaaijers, Rewizorski, & Arapova, 2021).

The coalition has become a leading representative of economies with high growth rates and growing populations, being often seen as the voice of emerging countries, as well as a challenger to Western dominance and institutions such as the World Trade Organization (WTO) and the International Monetary Fund (IMF) in global politics and economic power (Maji, 2021). Reform of the United Nations (UN) is frequently advocated to address the need for these institutions to become more inclusive of emerging economies. As noted in the fourteenth BRICS Summit's Beijing Declaration:

> We (...) reiterate the call for reforms of the principal organs of the United Nations. We recommit to instill new life in the discussions on reform of the UN Security Council and continue the work to revitalize the General Assembly and strengthen the Economic and Social Council. (MFA, 2022, para. 13)

In the same Declaration is stated that: "China and Russia reiterated the importance they attach to the status and role of Brazil, India and South Africa in international affairs and supported their aspiration to play a greater role in the UN" (MFA, 2022, para. 13).

In the sphere of the WTO, the BRICS aim to promote equitable trade practices while voicing their opposition to protectionist policies that disproportionately impact emerging economies. They have collectively called for the preservation of the multilateral trading system and have pushed for reforms that address the inequities faced by developing nations (MFA, 2022). At the G20, BRICS leaders meet on the sidelines to coordinate their position, and

the group has advocated for more inclusive and sustainable economic growth, financial stability, and the reform of international financial institutions to improve the realities of the global economy (Kirton & Larionova, 2022).

Albeit the group's cooperation narratives, Beeson and Zeng (2018) argue that the impact of BRICS on global governance has been lackluster. They highlight the absence of a clear, unified position among the BRICS nations, pointing out the creation of the AIIB by China despite the existence of the NDB. Structural problems within BRICS are evident, especially regarding China's dominant presence in the international order, suggesting that any BRICS initiative will likely reinforce China's position. Additionally, disputes between China and India further complicate BRICS' cohesion. The two nations not only have strained relations but also maintain partnerships with each other's strategic rivals, with India's involvement in the Quadrilateral Security Dialogue (QUAD) strategy for the Indo-Pacific and China's cooperation with Pakistan being prime examples. The authors maintain that: "(...) even if some of the BRICS are pushing for similar reforms in the prevailing global order, they are not necessarily a result of the collective efforts or thinking of the BRICS, but of individual national interests (Beeson & Zeng, 2018, p. 10).

4.1 Initiatives on ICT development and Internet governance

The primary focus of the BRICS in shaping digital governance is to adhere to the principles of non-interference and sovereignty, aiming to uphold international information security and advocating for its inclusion in International Law at the UN level (Ignatov & Zinovieva, 2024). The group has undertaken several joint initiatives to advance ICT development, aiming to leverage technology for economic growth, innovation, and improved quality of life. An important initiative is the BRICS Institute of Future Networks (BIFN), dedicated to collaborative research and development in next-generation network technologies such as 5G, 6G, and the Internet of Things (IoT). The BIFN was first proposed in 2016 as part of the BRICS ICT Development Action Plan. In 2017, a specific action plan was created following a focus group organized by China and India. The initiative was officially approved in 2018, along with the establishment of a council mechanism (BIFN, 2022). At the BRICS Summit of 2018 in Brasilia, China and South Africa proposed the BRICS Partnership on New Industrial Revolution (PNIR), focusing on areas such as smart manufacturing, industrial automation, and advanced materials, aiming to modernize industries, enhance productivity, and promote sustainable development (BPIC, 2022). The Digital BRICS Task Force (DBTF) was also proposed during the 2018 BRICS Summit to enhance digital cooperation in

the digital economy, cybersecurity, and innovation. The relevance of the DBTF lies in the coordination of digital policy, data protection, and internet sovereignty (Belli, 2021). Moreover, the Summit delineated the BRICS Science, Technology, and Innovation Work Plan spanning from 2019 to 2022, alongside the institutionalization of the DBTF and the introduction of the Innovation BRICS Network (iBRICS Network) (BRICS Information Centre, 2019).

4.2 China's digital investment in the BRICS

It has become clear that China plays a crucial role in guiding the joint efforts of the BRICS nations towards digital security, particularly concerning digital infrastructure and the advancement of high-tech industries, despite the varying ways in which each BRICS member engages with and aligns with China. (Ignatov & Zinovieva, 2024).

Chinese technology's presence in BRICS countries is a key aspect of the broader strategy to promote its model of Internet governance. The advancement in integrating its telecommunications and digital infrastructure, primarily through companies such as Huawei and ZTE, and its efforts in promoting initiatives like the Digital Silk Road (DSR) as part of the BRI, exemplify the country's proactive approach to driving economic and technological progress while concurrently enhancing its influence over global digital landscapes. This integration allows China to propagate its technological standards and governance model, while host countries must balance the resulting economic and technological benefits with its potential impacts (Hussain, Hussain, Khan, & Imran, 2024).

The introduction of Chinese technology is understood differently by the BRICS countries. In the case of Russia, collaboration with China on the digital infrastructure and technology sector has been a significant aspect of their bilateral relations. Besides satellite technology collaboration, Huawei's development of the 5G network has been a major player, striking deals with Beeline and MTS, which has raised international concern regarding the war in Ukraine and the potential Chinese assistance to Russia (Kolodii, Pili, & Crawford, 2024).

China has made significant digital investments in India, especially in sectors such as telecommunications, with companies like Huawei and ZTE. However, both companies were barred from participating in 5G trials after the Indian government's refusal (BBC, 2021). On the e-commerce front, Alibaba, owned by Ant Group, recently sold its shares in Paytm, one of India's largest digital payment platforms (He, 2023). Tencent had to remove its games from the Indian market in 2020, following the ban on Chinese apps (Kashyap,

2023). Chinese smartphone and computer brands Xiaomi, Oppo, Vivo, and Lenovo were all accused of tax evasion (Mallick, 2023). As of 2024, there are reports about Chinese companies having the opportunity to expand in the Indian market through Joint Ventures (JVs) (The Economic Times, 2024). As outlined before, India's geopolitical tensions and border disputes with China have led to mutual distrust, prompting India to reduce reliance on Chinese technology and promote domestic alternatives. India's alliance with the US, Japan, and Australia for an Indo-Pacific strategy to contain the BRI is also an example of a significant tension point (Choong, 2019).

In 2023, Brazil has garnered attention on the international stage by actively pivoting towards enhanced cooperation with China, starkly contrasted with the country's previously skeptical stance on Chinese investments under former President Bolsonaro's administration (Sousa, Abrão & Porto, 2023). Highlighting a new era in bilateral relations, President Xi and the Brazilian government have inked 15 agreements focusing on pivotal areas such as 5G technology, semiconductors, the Internet of Things (IoT), and digital security (Paraguassu, 2023).

As South Africa's primary trading counterpart, China is pivotal, evidencing a strong economic relationship between the two nations. China's substantial financial engagements primarily focus on the development of the energy sector and infrastructural enhancements within South Africa. This collaboration is highlighted by South Africa's reliance on China for cost-effective hardware solutions, solidifying and deepening their economic connections (Gouvea, Kapelianis & Li, 2020).

5. Discussion

In his speech at the BRICS Business Forum in South Africa, Xi Jinping highlighted that the next decade will see a significant transformation in the global governance system, moving towards multi-polarity and increased economic globalization despite current setbacks, also pointing out that geopolitical tensions, terrorism, and rising unilateralism threaten multilateralism and global trade. Xi also emphasized that the international community now faces critical choices regarding cooperation versus confrontation and openness versus protectionism and that BRICS countries should adapt to these changes, seize development opportunities, and work together to foster new international relations and a shared future for humanity (Xi, 2018). President Xi's interventions, combined with the expansion of the BRICS, which included several developing economies, sent the message that China views the BRICS as an effective tool to challenge the global governance

system (Lukin & Fan, 2019). However, the challenge to the governance system may not necessarily create a new international order but instead replicate the existing one (Freire, 2018).

As previously observed, China considers digital sovereignty a crucial aspect of internet governance and a primary foreign policy objective. This supports the aim of creating a shared community in cyberspace to reinforce digital sovereignty and information security (Ignatov & Zinovieva, 2024). The commitment to a state-centric digital sovereignty approach is reflected in its comprehensive regulatory framework aimed at controlling and monitoring online activities within its borders. Laws such as the CL and the PIPL are designed to enhance the state's control over data and information flows, ensuring that domestic internet infrastructure aligns with national security interests. This legal framework not only bolsters internal information security but also sets a precedent for other nations looking to assert greater control over their digital environments. China actively promotes its vision of cyber governance on the international stage through various diplomatic channels and strategic partnerships. In forums like the UN, the country supports the principle of non-interference in the digital affairs of sovereign states and emphasizes that each country should have the authority to regulate cyberspace.

China's investment in the BRICS highlights its strategy of building a coalition of emerging economies supporting a multipolar Internet governance approach. The country holds significant influence within the group, as it surpasses their combined economies: "Despite the BRICS countries combined accounting for over 20 % of global GDP, China's GDP is higher than the four others combined. Additionally, Beijing often has more in common with advanced economies than with developing countries" (Duggan, Hooijmaaijers, Rewizorski & Arapova, 2021, p. 472). By fostering cooperation among BRICS nations, the aim is to create a counterbalance to Western-dominated cyber norms and promote a more diversified and inclusive global digital order, which not only enhances China's influence in shaping global cyber policies but also encourages other countries to adopt similar stances on digital sovereignty and cybersecurity. Besides the divisions within the BRICS countries, especially between China and India, the Chinese perspectives are reflected in economic institutions such as the AIIB and the NDB (Cardoso, 2023).

It can be argued that the instrumentalization of the concept of digital sovereignty has the opposite effect of granting autonomy to the Global South, as it is used to perpetuate and reinforce existing power structures (Fischer, 2022). While digital sovereignty rhetoric promotes national control over

digital infrastructures and data, it often results in the consolidation of power by dominant states and multinational corporations. For the Global South, this translates into increased dependency on technology and infrastructure provided by other nations, such as China and the United States. Furthermore, the export of digital sovereignty models can impose regulatory standards and political alignments that may not suit the local contexts and needs of developing nations, thereby entrenching existing geopolitical hierarchies.

Nevertheless, after briefly analyzing the countries' responses towards Chinese investment and technology, significant disparities become evident. Russia exhibits substantial cooperation with China in the digital sector, aligning closely with Chinese technological policies. In contrast, India has set clear boundaries to reduce dependency on Chinese technology by modernizing its domestic infrastructure and fostering innovation to maintain strategic autonomy. Brazil and South Africa, meanwhile, primarily focus on their infrastructure development. Both nations recognize the benefits of Chinese investment in bridging their infrastructural gaps but face challenges in articulating and implementing a coherent vision for digital sovereignty due to political instability. Brazil's fluctuating political landscape hinders the consistent pursuit of long-term digital strategies, while South Africa grapples with socio-economic issues that divert attention from comprehensive digital policymaking.

Joint BRICS initiatives like the DBTF are relatively recent, making it difficult to assess their long-term effect, so these initiatives may struggle to achieve the significant impact they aim for when announced at the Summits. In the absence of cohesive collaboration, cooperation among BRICS countries may tend to shift towards bilateral arrangements rather than multilateral ones, potentially diluting the overall effectiveness of these initiatives.

These disparities show the complex background of digital sovereignty within the BRICS. Individually, while some countries embrace Chinese digital investment to varying degrees and align with Chinese policymaking, others actively seek to diversify their technological partnerships and bolster domestic capabilities to mitigate reliance on external powers. However, within the BRICS group context, there's collective advocacy for multilateralism that emphasizes sovereign control over digital spaces. This stance enables the BRICS to present a distinctive front in international forums, challenging Western-dominated narratives and promoting an alternative vision of Internet governance.

6. Conclusion

The purpose of the presented analysis was to determine how the Chinese conception of digital sovereignty aligns with the BRICS agenda for global internet governance, the main argument being that China's economic and diplomatic position grants significant influence despite divisions within the group.

China's role is bolstered by technological leadership in various key domains such as 5G networks, and e-commerce, which enables it to influence standard setting and policies. The effect of Chinese tech giants such as Alibaba and Huawei on the digital economy is also noteworthy. Furthermore, China's active involvement in the development of digital infrastructure is evident through initiatives like the BRI digital arm, the DSR. As shown by the analysis of some of the Chinese cybersecurity laws, data protection measures, and the approach to digital sovereignty, the Chinese conception of sovereignty aims to uphold their political structure, safeguard the integrity of China's governance system, and defend against external influences. Digital sovereignty is a fundamental principle guiding China's approach to interstate relations in cyberspace, as it emphasizes domestic information governance and core principles of non-interference and self-determination.

The cooperation between the BRICS countries holds promise for mutual benefits, particularly through initiatives like the NDB. However, the BRICS face significant weaknesses as a unified group, including the absence of a binding framework or enforcement mechanisms to ensure compliance with collective decisions. The economic disparities and varied levels of technological advancement among these countries add to the complexity of forming a unified strategy. Moreover, geopolitical tensions, especially between China and India, can hinder collaboration within the group. Historical conflicts and border disputes contribute to a lack of trust, which complicates joint initiatives and policy alignment, as competing regional interests can lead to fragmented approaches to digital sovereignty. Each BRICS country has its strategic priorities and domestic pressures, making it difficult to reach a consensus on collective actions.

Nonetheless, China's focus on digital investments and infrastructure development drives much of the BRICS agenda in this area, adapting to the prevailing issues. The unequal footing can lead to a perception that BRICS is more of a platform for advancing China's strategic goals rather than a truly collaborative partnership. Reliance on Chinese technology and infrastructure can result in economic dependence, reducing the bargaining power of other

BRICS countries and limiting their ability to develop independent digital strategies.

Overall, while each BRICS has unique priorities and challenges, they collectively contribute to advancing digital security and infrastructure in several international forums and joint initiatives. Driven by key players like China, they aim to reshape global governance, enhance digital sovereignty, and promote economic development. However, the risk remains that these efforts might replicate existing global power structures rather than create a new, more equitable international order.

Data de receção: 31/07/2024
Data de aprovação: 14/11/2024

References

Ayodele, O. (2022). Big Tech: Not-so-Simple Politics. In P. G. Sampath, & F. Tregenna, *Digital Sovereignty: African Perspectives* (pp. 99-109). Johannesburg: DSI/NRF South African Research Chair in Industrial Development.

BBC. (2021, may). *Huawei and ZTE left out of India's 5G trials*. Retrieved from BBC: https://www.bbc.com/news/business-56990236

Beeson, M., & Zeng, J. (2018). The BRICS and global governance: China's contradictory role. *Third World Quarterly*, 1-18.

Belli, L. (2021). Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *AJIC 28*, 1-14.

Belli, L., & Jiang, M. (2024). Digital Sovereignty in the BRICS: Structuring Self-determination, Cybersecurity, and Control. *Cambridge University Press*, 1-23.

BIFN. (2022). *About BIFN*. Retrieved from BRICS Institute of Future Networks: https://www.bifn.org/about.html

Blanc, F., & Poznanski, F. (2018, january). *Connecting Europe to Latin America: a revolution in Internet governance*. Retrieved from Internet Sans Frontières: https://internetwithoutborders.org/connecting-europe-to-latin-america-a-revolution-in-internet-governance/

BPIC. (2022). *BPIC*. Retrieved from BRICS PartNIR Innovation Center: https://www.bricspic.org/En/Pages/Home/AboutDetail.aspx?rowId=2&classId=1

BRICS Information Centre. (2019). *Brasilía Declaration*. Retrieved from BRICS Information Centre – University of Toronto: http://www.brics.utoronto.ca/docs/191114-brasilia.html

Broeders, D., & Berg, B. v. (2020). *Governing Cyberspace – Behavior, Power, and Diplomacy*. In D. Broeders, & B. v. Berg, Governing Cyberspace – Behavior, Power, and Diplomacy (pp. 1-18). Maryland: Rowman & Littlefield.

Brown, K. (2020). Domestic and Foreign Policy-Making in China. In T. Inoguchi, *The SAGE Handbook of Asian Foreign Policy* (pp. 423-442). London: SAGE Publications.

Cardoso, D. (2023). O Paradoxo dos BRICS: Uma proposta de revisionismo por cumprir. In A. Sousa Lara, *Tempos de Subversão* (pp. 269-283). Lisboa: MGI.

CGI.BR. (2014). *Lei do Marco Civil da Internet no Brasil*. Retrieved from Comité Gestor da Internet no Brasil: https://www.cgi.br/lei-do-marco-civil-da-internet-no-brasil/

China State Council. (2011, setembro). *China issues white paper on peaceful development*. Retrieved from Embaixada da República Popular da China: http://pt.china-embassy.gov.cn/pot/zgabc/201109/t20110907_2959627.htm

China State Council. (2022). *China issues white paper on peaceful development*. Beijing: Information Office of the State Council.

Chinese Academy of Cyberspace Studies. (2023). *China Internet Development Report 2020*. Singapore: Springer.

Choong, W. (2019). The return of the Indo-Pacific strategy: an assessment. *Australian Journal Of International Affairs 73*(5), 1-16.

Cooper, A. F. (2020). China, India and the pattern of G20/BRICS engagement: differentiated ambivalence between 'rising' power status and solidarity with the Global South. *Third World Quarterly 42*(9), 1945-1962.

Creemers, R. (2020). China's Conception of Cyber Sovereignty – Rhetoric and Realization. In D. Broeders, & B. v. Berg, *Governing Cyberspace – Behavior, Power, and Diplomacy* (pp. 107-144). Maryland: Rowman & Littlefield.

Duggan, N., Hooijmaaijers, B., Rewizorski, M., & Arapova, E. (2021). Introduction: 'The BRICS, Global Governance, and Challenges for South–South Cooperation in a Post-Western World'. *International Political Science Review 43*(4), 469-480.

Ermoshina, K., & Musiani, F. (2017). Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. *Media and Communication 5*(1), 42-53.

Fischer, D. (2022). The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Z Politikwiss*, 383-402.

Freire, M. R. (2018). Political dynamics within the BRICS in the context of multilayered global governance. In M. Larionova, & J. J. Kirton, *BRICS and Global Governance* (pp. 70-88). New York: Routledge.

Gong, X. (2019). The Belt & Road Initiative and China's influence in Southeast AsiaC. *The Pacific Review 4*, 635-665.

Gouvea, R., Kapelianis, D., & Li, S. (2020). Fostering intra-BRICS trade and investment: The increasing role of China in the Brazilian and South African economies. *Thunderbird Int. Bus. Rev. 62*, 17-26.

Griffiths, J. (2019). *The GreatFirewall of China: How to Build andControl an AlternativeVersion of the Internet*. London: Zed Books Ltd.

Hanna, N. K., & Qiang, C. Z.-W. (2010). China's Emerging Informatization Strategy. *Journal of the Knowledge Economy*, 128-164.

He, L. (2023, february). *Alibaba sells remaining stake in top Indian online payment provider Paytm*. Retrieved from CNN Business: https://edition.cnn.com/2023/02/13/tech/alibaba-exit-paytm-india-tech-market-intl-hnk/index.html

Hussain, F., Hussain, Z., Khan, M. I., & Imran, A. (2024). The digital rise and its economic implications for China through the Digital Silk Road under the Belt and Road Initiative. *Asian Journal of Comparative Politics 9*(2), 238-253.

Ignatov, A., & Zinovieva, E. (2024). BRICS Agenda for Digital Sovereignty. *RIAC*, 1-7.

Jelinek, T. (2023). *The Digital Sovereignty Trap – Avoiding the Return of Silos and a Divided World*. Cambridge: Springer.

Jiang, M. (2021). Cybersecurity Policies in China. In L. Belli, *CyberBRICS Cybersecurity – Regulations in the BRICS Countries* (pp. 183-226). Rio de Janeiro: Springer.

Kashyap, H. (2023, jun). *Tencent Looking At India Comeback With Undawn Game Launch*. Retrieved from Inc42: https://inc42.com/buzz/tencent-looking-at-india-comeback-undawn-game-launch/

Kirton, J., & Larionova, M. (2022). The First Fifteen Years of the BRICS. *International Organisations Research Journal 17*(2).

Kolodii, R., Pili, G., & Crawford, J. (2024, march). *Hi-Tech, High Risk? Russo-Chinese Cooperation on Emerging Technologies*. Retrieved from RUSI: https://www.rusi.org/explore-our-research/publications/commentary/hi-tech-high-risk-russo-chinese-cooperation-emerging-technologies

Koty, A. C. (2020, july). *What is the China Standards 2035 Plan and How Will it Impact Emerging Industries?* Retrieved from China Briefing: https://www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/

Lee, J. (2022). Cyberspace Governance in China Evolution: Features and Future Trends. *Asie.Visions 129, Ifri, July 2022.*

Lukin, A., & Fan, X. (2019). What is BRICS for China? *Strategic Analysis 43*(6), 620-631.

Maji, B. (2021). BRICS Towards The Multipolar World. *RJPSSs XLVII* (1) , 24-31.

Mallick, S. (2023, jul). Xiaomi, Oppo, Vivo and Lenovo under probe over alleged GST evasion. Retrieved from The Economic Times: https://economictimes.indiatimes.com/industry/telecom/telecom-news/xiaomi-oppo-vivo-and-lenovo-under-probe-over-alleged-gst-evasion/articleshow/102020299.cms

Mazenda, A., & Ncwadi, R. (2016). The rise of BRICS development finance institutions: A comprehensive look into the New Development Bank and the Contingency Reserve Arrangement. *African East-Asian Affairs*, 96-123.

MC, A., & Shanmugam, K. (2023). Unified Payment Interface—Taking India to the next generation in payments. *Journal of Information TechnologyTeaching Cases*, 1-16.

MFA. (2022, june). *XIV BRICS Summit Beijing Declaration*. Retrieved from Ministry of Foreign Affairs of the People's Republic of China: https://www.fmprc.gov.cn/eng/wjdt_665385/2649_665393/202206/t20220623_10709037.html

Moraes, R. F. (2020). Whither Security Cooperation in the BRICS? Between the Protection of Norms and Domestic Politics Dynamics. *Global Policy*, 1-9.

O'Neill, A. (2024, july). *Gross domestic product (GDP) of the BRICS countries from 2000 to 2029*. Retrieved from Statista: https://www.statista.com/statistics/254281/gdp-of-the-bric-countries/

Paraguassu, L. (2023, april). *Brasil abre caminho com China para parceria em tecnologia de semicondutores*. Retrieved from CNN Brasil: https://www.cnnbrasil.com.br/tecnologia/brasil-abre-caminho-com-china-para-parceria-em-tecnologia-de-semicondutores/

PIPL. (2021). PIPL. Retrieved from Act Summary: https://personalinformationprotectionlaw.com/PIPL/hello-world/

Quan, E. (2022). Censorship Sensing: The Capabilities and Implications of China's Great Firewall Under Xi Jinping. *Sigma: Journal of Political and International Studies 39*(4), 19-31.

Rezende, L. V., & Lima, M. R. (2015). Governança na internet: um estudo sobre o Marco Civil brasileiro. *Palabra Clave 19*(1), 133-155.

Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Hoover Institution*.

Sousa, A., Abrão, R., & Porto, L. (2023). A China na política externa do terceiro governo Lula: cem dias de reconstrução. *Rev. Conj. Aust. 14*(68), 150-162.

Stadnik, I. (2019, may). *A closer look at the "sovereign Runet" law*. Retrieved from School of Public Policy at Georgia Institute of Technology: https://www.internetgovernance.org/2019/05/16/a-closer-look-at-the-sovereign-runet-law/

The Economic Times. (2024, may). *Chinese companies may be permitted to dilute stakes in JVs with Indian partners*. Retrieved from The Economic Times: https://economictimes.indiatimes.com/news/economy/policy/chinese-companies-may-be-permitted-to-dilute-stakes-in-jvs-with-indian-partners/articleshow/110583169.cms?from=mdr

Wang, A. (2020). Cyber Sovereignty at its boldest: A Chinese perspective. *Ohio St. Tech. LJ*, 396-466.

Xi, J. (2018, july). *Full text of President Xi's speech at BRICS Business Forum in South Africa*. Retrieved from China Daily: http://www.chinadaily.com.cn/a/201807/26/WS5b5a80e3a31031a351e90857.html

About the author

INÊS RITO completed her master's degree in Chinese Studies at the University of Aveiro and is a PhD student in International Relations at the Institute of Social and Political Sciences of the University of Lisbon (ISCSP-ULisboa), currently working under the FCT-CCCM partnership scholarship. Her current research focuses on internet governance and China's promotion of digital sovereignty at the United Nations.

[ORCID ID: https://orcid.org/0009-0000-7306-4169]

Sobre a autora

INÊS RITO concluiu o mestrado em Estudos Chineses na Universidade de Aveiro e é doutoranda em Relações Internacionais no Instituto Superior de Ciências Sociais e

Políticas da Universidade de Lisboa (ISCSP-ULisboa), atualmente ao abrigo da bolsa de parceria FCT-CCCM. A sua investigação atual centra-se na governança da Internet e na promoção da soberania digital pela China nas Nações Unidas.

[ORCID ID: https://orcid.org/0009-0000-7306-4169]