liinc EM REVISTA

ARTIGO/ARTICLE

China's Approach to Cybersecurity and Information Integrity[1]

A Abordagem da China em Relação à Cibersegurança e à Integridade da Informação

Yi Shen
Fudan University.
Shanghai, China.

Shuyan Zhang
Fudan University.
Shanghai, China.

Ingrid Torquato Oliveira
Universidade de São Paulo (USP).
São Paulo, SP, Brasil.

Correspondência para/Correspondence to
Ingrid Torquato Oliveira: ingridtorquato@usp.br

PERIÓDICO / JOURNAL
ISSN 1808-3536
@liinc-emrevista
https://revista.ibict.br/liinc/index

FLUXO EDITORIAL / EDITORIAL PROCESS
Editores do Artigo / Article Editors
Fábio Guedes Gomes - José Medeiros
Marco Schneider - Chen Lan

Editores / Editors
Marco Schneider
Gustavo Saldanha
Fábio Gouveia

Cronologia / Timeline
Recebido / Received: 01/12/2025
Aprovado / Approved: 31/01/2025
Publicado / Published: 23/06/2025

Como citar / How to cite: SHEN, Yi; ZHANG, Shuyan; OLIVEIRA, Ingrid. sA. China's Approach to Cybersecurity and Information Integrity. *In*: *Liinc em Revista*, v. 21, n. 01, e7537. Disponível em: https://revista.ibict.br/liinc/article/view/7537. Acesso em: 27 jun. 2025.

[1] The *Liinc em Revista* journal had the support of **FAPERJ** for the publication of this article

RESUMO: A integridade da informação tem se tornado um dos temas centrais da cibersegurança. No caso da China, manter a soberania digital no ciberespaço significa equilibrar as contradições entre a segurança nacional e o desenvolvimento da economia digital. O país foi um dos pioneiros em propor o conceito de soberania cibernética e o primeiro a sugerir a soberania digital baseada nesse conceito. Por um lado, a China está comprometida em construir um padrão igualitário e ordenado para a transmissão transfronteiriça de dados. Por outro, também tem se dedicado a lidar com os riscos da desinformação para a soberania nacional e a segurança da população. Este artigo apresenta a experiência prática da China na governança da segurança de dados, assim como uma análise do papel do país na cooperação em cibersegurança dos Brics.

Palavras-chave: China; cibersegurança; integridade da informação; soberania cibernética.

ABSTRACT: Information Integrity has become one of the most important subjects of cybersecurity. China is one of the pioneers into proposing the concepts of cyber sovereignty and digital sovereignty, to balancing the contradictions between national security and the development of the digital economic. On the one hand, China is committed to building an equal and orderly cross-border data transmission pattern. While on the other hand, China is also committed to dealing with the risks of disinformation to sovereignty and people's security. This paper introduces China's practical experience in data security governance and analyzes China's role in BRICS cybersecurity cooperation.

Keywords: China; cybersecurity; information integrity; cyber sovereignty.

INTRODUCTION

The concept of Information Integrity has gained significant importance in both technological and social contexts, referring to the accuracy, consistency, and reliability of information and data throughout its lifecycle. It ensures that information remains unaltered, trustworthy, and free from unauthorized modifications, whether due to technical errors, malicious attacks, or deliberate manipulation (Baskerville, 1993). This concept is rooted in computer science but has expanded to address broader societal challenges and technological advancements (Wang; Strong, 1996), such as combating disinformation and ensuring equitable access to truthful information. Its dual nature makes it a critical issue in both technological and sociopolitical domains.

In computer science, Information Integrity is a fundamental principle of data management and cybersecurity. Its main goal is to shield data from loss, corruption, and illegal alteration. Access controls, which limit who can alter or access data to prevent tampering; data validation, which ensures that data inputs meet predetermined criteria to prevent errors; checksums and hash functions, which detect changes or corruption in data during storage or transmission; and backup and recovery systems, which guarantee that data can be restored to its original state in the event of corruption or loss. Since even little data discrepancies can result in serious system failures or security breaches, information integrity is intimately related to database management, network security, and software engineering in this context (Redman, 1998; Von Solms; Van Niekerk, 2013).

Beyond its technical definition, Information Integrity has profound social implications. Ensuring the integrity of information is key to preserving faith in public institutions, the media, and democratic processes in a time of widespread disinformation, fake news, and digital manipulation. According to the "United Nations Global Principles for Information Integrity", information integrity

> […] entails a pluralistic information space that champions human rights, peaceful societies and a sustainable future. It holds within it the promise of a digital age that fosters trust, knowledge and individual choice for all (United Nations, 2024a, p.3).

Combating disinformation by promoting accurate and verified information to refute false narratives; protecting vulnerable groups by ensuring that campaigns to spread misinformation do not target marginalized communities; bolstering democratic processes by preventing the manipulation of elections and public discourse; and promoting media pluralism by fostering diverse and independent sources of information to prevent monopolistic control of narratives are some of the key social impacts (United Nations, 2024a; World Economic Forum, 2023; ČORBA et al., 2024; Brazil; Unesco, 2024). To ensure that information serves the public interest rather than private or malicious purposes, its social dimension highlights the need for global cooperation, regulatory frameworks, and public awareness to address these challenges.

Information Integrity is a cornerstone of cybersecurity. While cybersecurity broadly focuses on protecting systems, networks, and data from cyber threats, Information Integrity specifically addresses the accuracy and trustworthiness of data within those systems. The relationship between the two can be summarized as follows: cybersecurity measures, such as encryption and access

controls, ensure that data cannot be altered without authorization, thereby preserving its integrity; cybersecurity tools monitor for unauthorized changes or corruption of data, which directly impacts Information Integrity; and both concepts aim to build trust in digital systems by ensuring that data remains accurate, reliable, and secure. In essence, Information Integrity is a critical component of cybersecurity, as compromised data integrity can undermine the security and functionality of entire systems. Conversely, robust cybersecurity practices are essential for maintaining Information Integrity in an increasingly interconnected and digital world.

With the development of globalization and the advent of the era of artificial intelligence (AI), emerging economies and countries of the Global South are playing an increasingly important role in cyberspace governance. The attitude and practice of data governance adopted by developing countries such as China and Brazil will largely determine the development model of global governance in the digital age. Therefore, this article discusses the basic ideas and practical experiences on information integrity and cybersecurity from a Chinese perspective. Furthermore, it will also seek to discuss the potential of the two countries to jointly promote BRICS cybersecurity coordination on the basis of China-Brazil cooperation.

China's Understanding of Cyber Sovereignty and Information Integrity

From Cyber Sovereignty to Digital Sovereignty

China is one of the world's pioneers to put forward the concept of "cyber sovereignty". During the 10 years from the introduction of the Internet in China in 1994 to the adoption of the "Tunis Agenda for the Information Society" at the World Summit on the Information Society (WSIS) in 2005, concepts such as "cyber sovereignty" and "information sovereignty" have begun to appear in the domestic academic literature (Liao, 2024).

In Chin's view, "cyber sovereignty" includes the following meanings. First, national sovereignty should be applied to cyberspace. Second, each country can exercise sovereign jurisdiction over cyberspace within its territory, enjoying independence of formulation and implementation of laws and policies. Third, when it comes to cross-border coordination, "cyber sovereignty" is equal among different countries.

The concept of "cyber sovereignty" is compared with the "multi-stakeholder" model proposed by European and American scholars. The "multi-stakeholder model" emphasizes that individuals, enterprises, social organizations and governments in cyberspace share the right to govern cyberspace. Although this concept also includes state actors, it highlights the relative independence of cyberspace from state power. As a result, in practice, European and American countries use the concept of "multi-stakeholder" to assert that cyberspace is a field of free competition, and artificially resist developing countries, including China, to exercise jurisdiction over the sovereignty of cyberspace. This claim of developed countries has for some time created a false perception that European and American countries do not emphasize cyber sovereignty. While this misconception was corrected by the political security problems reflected in the 2016 US presidential election and the "Prism scandal".

Therefore, for China, building a cyber sovereignty order means adhering to the principle of sovereign equality while accommodating different social actors to participate in cyber governance. As can be

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7537, junho 2025.
https://doi.org/10.18617/liinc.v21i1.7537

seen from China's official documents over the years, the Chinese government has always tried to apply the principle of openness and cooperation to the principle of sovereign equality.

At the 2nd World Internet Conference in 2015, President Xi Jinping pointed that the principle of sovereign equality established in the U.N. Charter is the basic norm of contemporary international relations, and its principles and spirit should also be applied to cyberspace. In terms of cyberspace governance system, it should be multilateral and multi-party coordinated, with consultation of all the parties. Governments, international organizations, Internet companies, technical communities, non-governmental organizations and individual citizens should all play their roles (Xi, 2015).

In 2023, the World Internet Conference released "Cyber Sovereignty: Theory and Practice (Version 4.0)", which emphasizes the principles of sovereign equality and justice while advocating the principle of cooperation. This means that China is committed to respecting the cyber sovereignty of other countries and opposing cyber hegemony and interference in internal affairs. At the same time, China calls on all countries, international organizations and all sectors of society to participate in the Internet governance system and fully consider the interests of all parties (Internet Society of China, 2023).

Following this spirit, the Ministry of Foreign Affairs of China launched "Strategy for International Cooperation in Cyberspace" in March 2017. The proposal to oppose hegemony and to suppor countries' independent choice of development path is specifically interpreted as follows.

"Countries should not use ICTs to interfere in other countries' internal affairs, and should not use their own advantages to undermine the security of other countries' supply chains of ICT products and services" (China, 2017).

The document describes the spirit of multi-party cooperation as the "principle of co-governance"

> [...] highlight the role of governments, international organizations, Internet companies, technical communities, non-governmental organizations, and individual citizens to build an all-dimensional and multi-faceted governance platform… The international community should jointly manage and equitably distribute basic Internet resources, establish a multilateral, democratic and transparent global Internet governance system, and realize the sharing of Internet resources, shared responsibility and joint governance (China, 2017).

Based on the diverse application scenarios of the principle of sovereignty in cyberspace, various parties in the international community have put forward concepts such as "data sovereignty" and "digital sovereignty" in recent years.

"Data sovereignty" emphasizes the strategic value of data, and its essence is that in the era of big data, the strategic value of data is receiving unprecedented attention. Countries have actively explored the effective governance of data, trying to find a balance between ensuring security and promoting development. The "European Data Strategy" and the "European Data Governance Regulation Proposal" issued by E.U. in 2020 are the best showcases.

In 2020, the European Parliament published "European Digital Sovereignty", in which "digital sovereignty" was clearly defined as

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7537, junho 2025.
https://doi.org/10.18617/liinc.v21i1.7537

> Europe's ability to act independently in the digital world, which should be understood in terms of both protective mechanisms and defensive tools to promote digital innovation, including cooperation with non-EU companies.

This concept is proposed by the E.U. to maintain independence, competitiveness and leadership in the face of competition in the digital world, emphasizing the ability of countries to lead their own digital development.

In recent years, Chinese scholars have gradually formed and improved China's understanding of "digital sovereignty" and "data sovereignty" in the process of exchanges with European scholars.

Similar to "cyber sovereignty", Chinese scholars have pointed out that each country has the right to independently regulate the data collected and generated within its territory. The legal regulation of cross-border data should maintain the public international law order based on sovereign states, respect sovereign differences as a principle, take the United Nations and its international arbitration institutions and mutual legal assistance agreements between states as the main channels for dispute resolution, and achieve the implementation through equal participation of all countries sharing and governance of cross-border data (Zhai, 2018; Qi; Pan, 2015).

Some scholars have also analyzed the unique properties of introducing the concept of sovereignty into cross-border data transmission governance, including the blurring of sovereignty boundaries, the weakening of independence and the strengthening of interdependence among sovereigns in the Internet environment (Xiong; Wang, 2024). Others have also pointed out that, the digital sovereignty can be divided into three different aspects: the infrastructure layer, the application layer, and the core layer. Among them, the core layer, including political security and ideology security, is inviolable, while the infrastructure layer and the application layer are shareable and transferable, and the transferability and exclusivity of sovereignty are flexible and changeable with the development of international rules (Hao, 2016).

Two Components of Digital Sovereignty: Orderly Data Flow and Information Integrity

One of the most important aspects of data (digital) sovereignty is that it provides basic guidelines for cross-border data flows. China's approach to cross-border data flows is "orderly flow". First, it recognizes the need and importance of maintaining cross-border data flows. Second, data flow must follow the principle of equality, security, and order. Third, governments should play a leading role, focusing on maintaining the safety and reliability. Fourth, it encourages companies and other non-state actors to actively participate.

In terms of data storage and ownership, the entering of user-created data into the storage device does not mean that ownership of the data is unconditionally transferred to the owner of the device. Users who provide data have the right to ensure that the data is used properly and does not threaten their own interests, and have the ultimate sovereignty over the disposal of data. Any disposal of the data should be explicitly authorized by the user, especially when the data is being mined.

When it comes to the common development of digital economy, the goal of countries, especially developing countries, is not to block the free flow of data, or to divide the global cyberspace with sovereign barriers, but to ensure that all countries, including those whose technological capabilities

are temporarily vulnerable, will not have their legitimate interests harmed due to differences in capabilities. The goal pursued by sovereign states is that the use of data can promote the interests of the original providers of data, rather than becoming a tool for the excessive pursuit of self-interests by a few actors with technological advantages.

With regard to the value of data resources, China sees data as the common property of all humankind, which means it should benefit as many actors as possible. Advanced actors with technological advantages, whether countries, companies or any form of association, should not abuse their own advantages uncontrollably, threatening, squeezing or even depriving the legitimate rights and interests of weak actors (Shen; Yao, 2018).

China's understanding of data sovereignty, in addition to emphasizing the role of the state in data flow, is also reflected in China's commitment to combating and countering disinformation and balancing the boundaries of security and freedom in content and data governance processes.

"Disinformation" is distinguished from "misinformation" in its nature. "Disinformation" is defined as "intentional misinformation", which has three characteristics: false content, misleading intention and organization of action. These three characteristics mean that disinformation, while violating citizens' right to personal information, is also likely to cause social and cultural impact due to its scale of dissemination, ultimately affecting the management process of the state and government. Driven by AIGC technology, the cost of generating and disseminating disinformation has become lower, which makes the risk of disinformation more extensive (Yuan, 2022; Peng, 2022; Qi, 2024; Lu; Dang, 2024).

Considering the dissemination mechanism of disinformation, it can be roughly divided into two variables: technical factors and social factors. At the technical level, the anonymity of the Internet and social media and the speed and breadth of information dissemination allow false information to spread quickly and affect public perception. At the social level, unexpected public events and public opinion emotions may also promote the accelerated dissemination of disinformation, and disinformation can even be used as a geopolitical tool to pursue political interests (Sun, 2025; Yuan, 2022; Huang; Yao, 2024).

In view of the above characteristics of disinformation, Chinese scholars have put forward diverse governance strategies from multiple dimensions.

From the legal aspect, it is necessary to improve relevant laws and regulations, clarify the definition and punishment standards of false information, and strengthen legal sanctions against false information disseminators. For example, the introduction of "The Interim Measures for the Management of Generative Artificial Intelligence Services" provides a legal basis for the management of false information. Technological innovation is also seen as an important tool in the fight against disinformation. Through the development of advanced algorithms and artificial intelligence technology, the rapid identification and filtering of false information can be achieved (Chen; Ma; Ma, 2024; Hu, 2024; Zhang et al., 2024).

In addition, the importance of improving public media literacy was also emphasized. The ability of the public to think critically and distinguish misinformation is the key to resisting disinformation.

Through education and publicity, the whole society can strengthen the public's immunity to false information and reduce the possibility of its spread. At the same time, the government and media organizations should strengthen the release of authoritative information, refute rumors in a timely manner, and correct the public. Governments, enterprises, social organizations and citizens are encouraged to participate in the governance of disinformation and form a pattern of collaborative governance (He; Li, 2024; Guo; Wei; Liu, 2024; Nan, 2024).

In summary, as a pioneer of cyber sovereignty and digital sovereignty, China began to notice the important political impact of information and data on sovereignty in a quite early stage of Internet development. In the era of artificial intelligence, China's understanding of digital sovereignty and cyber sovereignty has become more comprehensive and complete. At the international level, China advocates an open, inclusive, free and equal data transmission order. At the same time and at the domestic level, it emphasizes dealing with disinformation through legal, technical and social methods. When China pursues information integrity, we always try to balance the contradiction between the two basic values of freedom and security. China believes that a good data governance model requires proper regulation of cyberspace and information content by state power on the basis of respecting the personal privacy of users and citizens. This is not only because individual freedom itself has limits, but also because the Chinese government believes that only by creating a good social environment through regulation can the development of cyberspace reach its full potential. In Chinese policy documents, we describe this kind of orderly and open online environment as "Qing Lang", which originally refers to clear and sunny weather. We use this concept to describe that citizens can use integrated information in a secure environment to achieve personal development.

CHINA'S PRACTICES OF DATA SECURITY GOVERNANCE

The Data Security Law of the People's Republic of China

In 2019, the Standing Committee of the National People's Congress ordered relevant government departments to jointly start drafting a data security law. After two rounds of deliberation, the "Data Security Law of the People's Republic of China" was adopted at the 29th meeting of the Standing Committee in 2021 and officially implemented in September. It is China's first specific law on data security.

The "Data Security Law" has seven chapters. Chapter I covers the general provisions, which determine the legislative background, basic definition and scope of application. Chapter II defines the relationship between data security and development. It emphasizes that both data utilization and data security protection share the same level of importance and encourages the rational and effective use of data according to law. Chapter III requires the establishment of a data security system, which gives classified protection according to the importance and sensitivity of data. It also calls for the establishment of review and monitoring warning mechanisms. Chapter IV defines the obligations of data security protection and clarifies the responsibilities of data processors and data security managers. Chapter V prescribes government data opening and government data security, and also emphasizes both security protection and open sharing. Chapter VI sets out the corresponding legal responsibilities, and Chapter VII is an appendix (China, 2021).

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7537, junho 2025.
https://doi.org/10.18617/liinc.v21i1.7537

The "Data Security Law" is a composite governance system established under the leadership of the government to coordinate security and development. As a developing country that needs to realize industrialization and informatization simultaneously, China will inevitably rely on the modernization model under the leadership of a strong political party to achieve its own rapid development. In other words, the protection of information integrity must be achieved with the help of digital sovereignty.

The biggest feature of the law is the precise protection of data security. China has established a data classification protection system, which protects data according to its importance in economic and social development, as well as the degree of harm to national security, public interests or the legitimate rights and interests of individuals and organizations once it is tampered with, damaged, leaked, illegally obtained or illegally used. The National Data Security Coordination Mechanism has led departments to formulate critical data catalogues to strengthen the protection of important data. Data relating to national security, the economy, people's livelihood, and major public interests have been identified as core data of the state, and a stricter management system is being implemented. All regions and departments shall, in accordance with the data classification and hierarchical protection system, determine the specific catalogues of important data of their respective regions, departments and related industries and fields, and give priority to the protection of the data included in the catalogues. These regulations show that the Chinese government is fully aware of the categories and characteristics of cyberspace data with great accuracy.

The purpose of the "Data Security Law" is not to impose one-side restrictions. The law clearly states that digital development and security are coordinated by the government. The government believes that data development and utilization have the potential to promote data security, and data security creates a necessary environment for data development. Therefore, the government is implementing a big data strategy, promoting the construction of data infrastructure and encouraging and supporting the innovative application of data in various industries. The law has also required all provinces of China to incorporate digital economy into their annual plan. The purpose of this law is to regulate rather than block cross-border data flows, to regulate rather than weaken the digital economy, and to protect rather than suppress the legitimate demands of Chinese citizens for their own data security (Shen, 2022).

The Regulation on Network Data Security Management

So far, China has issued the "Cybersecurity Law", the "Data Security Law" and the "Personal Information Protection Law", which constitute the basic structure of China's data security legal system. On September 30, 2024, the "Regulation on Network Data Security Management" was officially released, aiming to provide more detailed implementation paths and guidelines for the three laws, regulate the most prominent network data security issues at present, and fill the regulatory gap in the field of data security management in China.

The "Regulation on Network Data Security Management" first makes operational provisions on the protection of personal information, requiring data processors to ensure users' right to know and privacy when invoking, collecting and processing personal information. Second, the Regulation specifies the classified protection of data and sets out the priorities for the relevant regulatory authorities when assessing and grading the importance of data. Third, the Regulation clarifies the security requirements that need to be met in the process of outbound data transfer and require data

processors to take the initiative to declare their behaviors. Fourth, the Regulation stipulates the responsibilities of large network platform service providers, requiring large network platforms to comply with data security regulations and conduct annual reports. Fifth, the Regulation clarifies the supervision and management responsibilities of the national cyberspace administration department and clarify the scope of supervision and operation norms of the government (China, 2024).

The Regulation gives specific operational legal guidance on the current network data security protection work of China and its working scope is quite comprehensive. The object of the Regulation covers government departments and data service providers and the data security issues involved include personal information protection, cross-border data transmission and network platform services, which directly responds to the core issues facing the current data governance in China. For example, when it comes to the data used in artificial intelligence training, the Regulation requires that network data processors of generative artificial intelligence services should strengthen the security management of training data and processing activities and take effective measures to prevent and deal with network data security risks. Data processors need to strengthen the legal management to ensure the compliance of data collection, collecting only the data necessary to achieve the function of the model, auditing the data source and clarifying the authorization and legal basis of the data. In the process of data processing, advanced privacy protection technology should be adopted to reduce the risk of data leakage. In addition, the Regulation also requires generative AI services to conduct security reviews of the generated content to prevent the disclosure of sensitive information or the spread of harmful information, so as to achieve information integrity.

The Regulation continues the Chinese government's long-standing efforts to encourage digital innovation. The Regulation is not intended to restrict the legitimate business practices of online platforms and data service providers, but to minimize compliance costs for enterprises and promote a healthy development of the digital economy. Articles 4, 6 and 7 of the General Provisions emphasize that the government encourages the innovative application and circulation of online data in various industries and fields, encourages active participation in the formulation of international rules and standards and promotes international exchanges and cooperation. At the same time, the Regulation clearly supports relevant industry organizations to formulate norms for network data security behavior in accordance with the charter, strengthen industry self-discipline and guide users to strengthen network data security protection. The regulation has successfully combined network data security with industrial development. The general provision of the Regulation points out that the core task of the Regulation is to establish a bottom line for data security, but its essence is to provide a stable environment and a fair competition order for the development of the industry.

CHINA'S ROLE IN THE BRICS CYBERSECURITY COOPERATION

The emergence and development of the BRICS countries (Brazil, Russia, India, China, and South Africa) has provided a significant opportunity to reshape the paradigm of global cyberspace governance. Since these countries together account for a sizable portion of the world's population, economy, and digital market, it is impossible to dispute their impact on how digital governance will develop in the future. The BRICS nations make up more than 40.4% of the world's population (United Nations, 2024b) and provide almost 25% of its GDP (World Bank, 2023), without

considering the new member countries. They are rapidly growing their footprint in the digital sphere; Brazil and South Africa are becoming important participants in regional digital economies, while China and India lead in terms of Internet users and digital innovation. The historical dominance of Western nations, especially the United States, in global Internet governance is being challenged by the combined strength of BRICS. By advocating for a more inclusive and equitable approach, BRICS aims to address the digital divide and ensure that developing nations have a greater say in the rules and norms governing the digital world.

Digital sovereignty in the BRICS countries is crucial for ensuring the control and protection of strategic data, recognizing it as an essential resource for economic and social development. These countries have adopted data governance approaches aimed at preserving their self-determination in managing and regulating data processing, reflecting their significance in the global digital transformation landscape (Belli; Gaspar; Jaswant, 2024). As BRICS expands, the ideological convergence among its new members, particularly in nations like Iran, Saudi Arabia, and Egypt, enhances multilateral collaboration on digital sovereignty, cybersecurity, and cross-border information sharing. This growing unity paves the way for more effective promotion of shared values and interests on the global stage, including within key institutions like the UN (Ignatov, 2024). For effective governance, balancing income distribution, ensuring inclusiveness, and fostering international cooperation, particularly among the BRICS nations, are essential. Deepening BRICS cooperation on digital economy strategies, establishing information-sharing mechanisms, improving transparency, and addressing the socio-economic impacts of technological innovation, such as income inequality and workforce training, can ensure sustainable and inclusive growth (Shen, 2024).

As the largest economy and a global leader in digital innovation in the BRICS, China has been actively involved in the cybersecurity discussions among the BRICS countries. At the Coordinator Meeting held by Brazil in February 2025, the BRICS countries agreed to make AI governance one of the priority themes for the term. The Chinese MFA commented that China has always been committed to developing AI that is good for the people, safe and controllable, green and low-carbon, and inclusive. AI technology and data are the common wealth of humankind, and it should not and cannot be reduced to a tool for maintaining hegemony and pursuing advantages. The BRICS countries should help each other to ensure that all countries have equal rights, equal opportunities and equal rules, so that AI will benefit all countries.

China has introduced the "Global Data Security Initiative (GDSI)" in September 2020 (China State Council, 2020). China's aim for a cooperative and fair approach to global data governance is reflected in the GDSI. The initiative's basic principle is that data resources ought to be seen as the collective property of all people, not as a strategic resource that can be controlled by one country.

The spirit of the GDSI is based on several fundamental principles, including: collaborative governance, which emphasizes that international cooperation is necessary to establish rules and norms for data security that benefit all countries, not just a selected few; shared development, which advocates that data resources should be used to promote global development, particularly in the Global South, rather than being concentrated in the hands of a few powerful nations; and mutual respect and non-aggression, which states that nations should respect each other's data sovereignty and refrain from engaging in cyberattacks or data theft; and accountability, guaranteeing that both

governments and companies will become open about their data activities and held responsible for any data misuse (China State Council, 2020).

By advocating for data resources to be treated as the common property of all humankind, China positions itself as a counterbalance to the U.S.-centric model of data governance, which often prioritizes strategic competition over shared development. Within BRICS, China's emphasis on mutual respect, non-aggression, and collaborative governance resonates strongly with the member nations, particularly those in the Global South, who seek to reduce their dependence on Western technologies and establish a more balanced global cyberspace order. This leadership role not only strengthens BRICS' collective voice in international cybersecurity discussions but also underscores China's commitment to addressing the digital divide and promoting a multipolar world where developing nations have a greater say in shaping the rules of the digital age.

Chinese scholars have praised the GDSI as a groundbreaking effort to counter the hegemony of Western powers in cyberspace because it aligns with the broader goals of BRICS to create a multipolar world order where developing countries have a greater voice. The concept of "multilateralism" is crucial to this strategy, emphasizing the value of cooperation among sovereign nations. The initiative's focus on data security, which frames data as "the common property of humanity, " reflects China's intention to create public goods for global cyberspace governance and is consistent with the present trends of the information technology revolution (Shen, 2014; Shen, 2020).

To sum up, China is trying to bring its successful domestic experience of balancing cybersecurity and digital economy development to the international level. Building a solid foundation of cybersecurity among the BRICS countries will create a trustworthy and reliable environment for digital development. The BRICS countries can maximize their influence in global digital transformation only by closely cooperating with each other. China advocates a governance model of "Consultation, Contribution and Shared Benefits" (Gong Shang, Gong Jian, Gong Xiang). On the basis of respecting sovereign equality, China will coordinate cybersecurity policies, jointly promote the development of the digital economy and share the benefits of digitalization with BRICS members.

FINAL REMARKS

In the future, China will further strengthen its efforts in digital governance and uphold national security while encouraging the development of the digital economy. In terms of guiding principles, China will continue to adhere to its digital sovereignty and resolutely put an end to the negative impact of disinformation on the interests of the country and the people. In terms of institutional design, China will continue to improve its legal system on data security and formulate more specific and operational guidelines under the existing legal framework. Information Integrity will be coordinated among individual citizens, enterprises, social organizations and the government to form a governance model with extensive participation of all sectors of society.

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7537, junho 2025.
https://doi.org/10.18617/liinc.v21i1.7537

At the international level, with the rise of developing countries, China will deepen its cooperation with the Global South represented by the BRICS countries and further promote international cooperation on cybersecurity. China will take the GDSI as its guiding principle, fully respect the interests of other nations and regard data resources as the common property of all humankind. Under the GDSI framework, China's definition of cybersecurity and data security will be a type of security community. This means that China will build an open data security system based on the BRICS countries, so that all countries in the world can participate in this security community equally. This is also the biggest difference between China's security initiative and the one built by developed countries represented by the United States, which is exclusive and guided by a zero-sum game mentality.

2025 will witness the second 10 years of WSIS. In July, the WSIS+20 High-level Meeting will be held in Geneva, and in December, the UN General Assembly will hold a high-level meeting to conduct an overall review of the implementation of WSIS outcomes. The more important significance of this special point of time is that today's world has entered the era of vigorous development of artificial intelligence, and AI technology has made data governance and disinformation governance even more critical in a digital society.

In a world of rapid development of the digital economy where governance issues are becoming increasingly prominent, China will actively promote practical and effective cooperation. At present, China has put forward a series of international documents such as the "Global Development Initiative", the "Global Data Security Initiative" and the "Global Artificial Intelligence Governance Initiative", aiming to contribute China's wisdom to global development and international governance cooperation in the digital age. China has always believed that a global community of shared future in cyberspace, based on respect for the principle of sovereign equality, should and can be the object of joint efforts by all parties.

Liinc em Revista, Rio de Janeiro, v. 21, n. 01, e7537, junho 2025.
https://doi.org/10.18617/liinc.v21i1.7537

REFERENCES

BASKERVILLE, Richard. Information systems security design methods: Implications for information systems development. **ACM Computing Surveys (CSUR)**, United States, v. 25, n.4, p. 375-414, 1 dez. 1993. Disponível em: https://dl.acm.org/doi/10.1145/162124.162127. Acesso em: 24 Feb. 2025.

BELLI, Luca; GASPAR, Walter Britto; JASWANT, Shilpa Singh. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. **Computer Law & Security Review**, United Kingdom, v. 54, 2024. DOI: https://doi.org/10.1016/j.clsr.2024.106017. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364924000839?via%3Dihub. Acesso em: 24 Feb. 2025.

BRAZIL. Secretaria de Comunicação Social. UNESCO. 2024. **Possible Approaches to Promoting Information Integrity and Trust in the Digital Environment**: Integrity of Information and Trust in the Digital Economy. Brasília, DF, set. 2024. Disponível em: https://www.gov.br/mcom/pt-br/acesso-a-informacao/governanca/governanca-de-tic-1/documentos-g20/p3-g20-dewg-brasil-2024-possible-approaches-to-information-integrity.pdf. Acesso em: 24 fev. 2025.

CHEN, Qiyuan; MA, Liming; MA, Tingxi. Réngōng Zhìnéng Shēnwěi Jìshù duì Rènzhī Ānquán de Tiǎozhàn yǔ Yìngduì = [Challenges and Responses of Artificial Intelligence Deepfake Technology to Cognitive Security]. **Nánfāng Chuánméi Yánjiū** = [**Southern Media Research**], [China], v. 6, p. 23-32, 2024.

CHINA. Office of the Central Cyberspace Affairs Commission. **Zhōnghuá Rénmín Gònghéguó Wàijiāobù: Wǎngluò Kōngjiān Guójì Hézuò Zhànlüè** = [**International Cooperation Strategy on Cyberspace**]. [Beijing, China], 1 mar. 2017. Disponível em: http://www.cac.gov.cn/2017-03/01/c_1120552617.htm. Acesso em: 24 fev. 2025.

CHINA. **Zhōngguó guójiā shùjù ānquán zhǐdǎo yìjiàn** = [**China's proposal on the Global Data Security Initiative**]. [Beijing, China]: Central People's Government of the People's Republic of China, 2020. Disponível em: https://www.gov.cn/xinwen/2020-09/08/content_5541579.htm. Acesso em: 24 fev. 2025.

CHINA. The National People's Congress of the People's Republic of China. **Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ** = [**The Data Security Law of People's Republic of China**]. [Beijing, China], 2021. Disponível em: http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html. Acesso em: 24 fev. 2025.

CHINA. Government of the People's Republic of China. **Wǎngluò shùjù ānquán guǎnlǐ tiáolì** = [**Regulations on Cyberspace Data Security Management**]. [Beijing, China], 2024. Disponível em: https://www.gov.cn/zhengce/zhengceku/202409/content_6977767.htm. Acesso em: 24 fev. 2025.

ČORBA, Juraj; PLONK, Audrey; PERSET, Karine; IIDA, Yoichi. Evolving with Innovation: The 2024 OECD AI Principles Update. **OECD.AI Policy Observatory**, 20 maio 2024. The AI Wonk. Disponível em: https://oecd.ai/en/wonk/evolving-with-innovation-the-2024-oecd-ai-principles-update. Acesso em: 24 fev. 2025.

GOLDSMITH, Jack. Sovereign Difference and Sovereign Deference on the Internet. **The Yale Law Journal Forum**, p. 818-826, 18 mar. 2019.

GREEN, Erik; NOUWENS, Meia; NOUWENS, Veerle. **The Global Security Initiative: China's International Policing Activities**. London: International Institute for Strategic Studies, 2024. Disponível em: https://www.iiss.org/research-paper/2024/10/the-global-security-initiative-chinas-international-policing-activities/. Acesso em: 24 fev. 2025.

GUO, Hailing; WEI, Jinjin; LIU, Zhongshan. Shēngchéng Shì Réngōng Zhìnéng Xūjiǎ Xìnxī Xiétóng Gòngzhì Yánjiū = [Research on Collaborative Governance of Generative Artificial Intelligence Disinformation]. **Qingbao Zazhi** = [**Journal of Intelligence**], [China], v. 43, n. 9, p. 121-165, 2024.

HAO, Yeli. Wǎngluò Shìjiè de Yuánzéxìng yǔ Línghuóxìng — Sān Shìjiǎo Xià Wǎngluò Zhǔquán de Duìlì Tǒngyī = [Principle and Flexibility in the Cyber World: The Unity of Opposites in Cyber Sovereignty from Three Perspectives]. **Shàntóu Dàxué Xuébào (Rénwén Shèhuì Kēxué Bǎn)** = [**Journal of Shantou University (Humanities & Social Sciences Edition)**], [Shantou, China], v. 6, 2016.

HE, Yuhua; LI, Xia. Shēngchéng Shì Réngōng Zhìnéng Xūjiǎ Xìnxī Zhìlǐ de Xīn Tiǎozhàn jí Yìngduì Cèlüè - Jīyú Mǐnjié Zhìlǐ de Shìjiǎo = [New Challenges and Response Strategies for Generative Artificial Intelligence Disinformation Governance: A Perspective Based on Agile Governance]. **Zhìlǐ Yánjiū** = [**Governance Studies**], [China], v. 40, n. 4, p. 142-160, 2024. DOI: 10.15944/j.cnki.33-1010/d.20240618.001. Acesso em: 24 fev. 2025.

HU, Yong. Rengong zhineng qudong de xujia xinxi: xianzai yu weilai = [Artificial intelligence-driven misinformation: Present and future]. **Nanjing Social Sciences**, [Nanjing, China], p. 96-109, 2024. DOI: 10.15937/j.cnki.issn1001-8263.2024.01.011. Acesso em: 24 fev. 2025.

HUANG, Rihan; YAO, Haolong. Shùzì Shídài de Bóyì: Shēngchéng Shì Réngōng Zhìnéng duì Guójiā Yìshí Xíngtài Ānquán de Yǐngxiǎng = [The Game in the Digital Age: The Impact of Generative Artificial Intelligence on National Ideological Security]. **Guójiā Ānquán Lùntán** = [**National Security Forum**], v. 3, n. 6, p. 54-96, 2024.

IGNATOV, Alexander. BRICS expansion and prospects for BRICS cooperation in the digital economy. **Russian International Affairs Council**, [*s. l.*], 2024. Disponível em: https://cyberbrics.info/policy-brief-brics-expansion-and-prospects-for-brics-cooperationin-the-digitaleconomy/. Acesso em: 26 fev. 2025.

INTERNET GOVERNANCE FORUM. **Key Findings from the Internet Governance Forum 2024**. [*S. l.*], 2024. Disponível em: https://intgovforum.org/en/filedepot_download/305/28529. Acesso em: 24 fev. 2025.

INTERNET SOCIETY OF CHINA. **Wǎngluò Zhǔquán**: Lǐlùn yǔ Shíjiàn (4.0 Bǎn) = [**Cyber Sovereignty**: Theory and Practice (Version 4.0)]. [Beijing, China], 2023. Disponível em: https://cn.wicinternet.org/2023-11/09/content_36955448.htm. Acesso em: 24 fev. 2025.

LIAO, Fan. Shùzì Zhǔquán yǔ Quánqiú Shùzì Zhìlǐ [Digital Sovereignty and Global Digital Governance]. **Jìnán Xuébào (Zhéxué Shèhuì Kēxué Bǎn)** = [**Journal of Jinan University (Philosophy & Social Sciences Edition)**], [Jinan, China], v. 46, n. 7, p. 47-60, 2024.

LU, Jianping; DANG, Ziqiang. AIGC Shídài Xūjiǎ Xìnxī de Zhìzào Chuánbò yǔ Guójiā Ānquán jí Gōngmín Quányì de Wéihù = [The Production and Dissemination of Disinformation in the AIGC Era and the Maintenance of National Security and Citizens' Rights]. **Zhèjiāng Dàxué Xuébào (Rénwén Shèhuì Kēxué Bǎn)** = [**Journal of Zhejiang University (Humanities and Social Sciences)**], [Zhejiang, China], v. 54, n. 5, p. 42-58, 2024.

NAN, Ting. Shengcheng Shi Rengong Zhineng Xujia Xinxi de Fengxian yu Zhili Celüe Yanjiu = [Research on Risks and Governance Strategies of Generative Artificial Intelligence Disinformation]. **Zhongguo Chuanmei Keji** = [**China Media Technology**], [China], n. 8, p. 129-133, 2024. DOI: 10.19483/j.cnki.11-4653/n.2024.08.029. Acesso em: 24 fev. 2025.

PENG, Zhihui. Lun Zhōngguó Yǔjìng Xià Disinformation Gàiniàn de Duìjiē, Zhuǎnhuàn yǔ Chóngxīn Chǎnshì = [On the Alignment, Transformation, and Reinterpretation of the Concept of Disinformation in the Chinese Context]. **Qingbao Lǐlùn yǔ Shíjiàn** = [**Information Studies: Theory & Application**], [China], v. 45, n. 1, p. 1-10, 2022. DOI: 10.16353/j.cnki.1000-7490.2022.01.001. Acesso em: 24 fev. 2025.

QI, Aimin; PAN, Jia. Shùjù Quán, Shùjù Zhǔquán de Quèlì yǔ Dà Shùjù Bǎohù de Jīběn Yuánzé = [The Establishment of Data Rights, Data Sovereignty, and the Basic Principles of Big Data Protection]. **Sūzhōu Dàxué Xuébào (Zhéxué Shèhuì Kēxué Bǎn)** = [**Journal of Soochow University (Philosophy & Social Sciences Edition)**], [Jiangsu, China], n. 1, p. 64-70, 2015.

QI, Chenhang. Shēngchéng Shì Réngōng Zhìnéng de Xūjiǎ Xìnxī Fēngxiǎn Tèzhēng jí Qí Zhìlǐ Lùjìng = [Risk Characteristics and Governance Pathways of Generative Artificial Intelligence Disinformation]. **Qingbao Lǐlùn yǔ Shíjiàn** = [**Information Studies: Theory & Application**], [China], v. 47, n. 3, p. 112-120, 2024. DOI: 10.16353/j.cnki.1000-7490.2024.03.015. Acesso em: 24 fev. 2025.

REDMAN, Thomas. The impact of poor data quality on the typical enterprise. **Communications of the ACM**, [New York, United States], v. 41, n. 2, p. 79-82, 1 fev. 1998. Disponível em: https://dl.acm.org/doi/10.1145/269012.269025. Acesso em: 24 fev. 2025.

SHEN, Yi. Quánqiú wǎngluò kōngjiān zhìlǐ yǔ jīnzhū guójiā hézuò = [Global cyberspace governance and BRICS cooperation]. **International Observation**, [*S.l.*], v. 4, p. 145-157, 2014.

SHEN, Yi. Jīyú zhǔquán píngděng yuánzé de shùjù zhìlǐ: Quánqiú wǎngluò kōngjiān zhìlǐ liángxìng biànhuà de xīn qūshì = [Data governance based on the principle of sovereign equality: New trends in the positive transformation of global cyberspace governance]. **China Information Security**, [China], v. 11, p. 71-74, 2020.

SHEN, Yi. Shuju Anquan Fa wei Shuzi Jingji Fazhan Tigong Anquan Baozhang = [The Data Security Law Provides Security Guarantees for the Development of the Digital Economy]. **Jinrong Bolan** = [**Financial Review**], [China], n. 6, p. 56-57, 2022.

SHEN, Yi. Digital Economy and Pragmatic Cooperation Among BRICS. **IPEA**, Brasilia/DF, 2024. Disponível em: https://portalantigo.ipea.gov.br/agencia/images/apresentacoes/forum_academico_brics/Shen_Yi_Digital_Economy_and_Pragmatic_Cooperation_Among_BRICS.pdf. Acesso em: 26 fev. 2025.

SHEN, Yi; YAO, Xu. Dàguó Zhànlüè Hùxìn yǔ Kuàjìng Shùjù Liúdòng Guǎnlǐ Xīn Móshì Tànsuǒ: Yǐ "Shùjù Zhǔquán" wéi Héxīn Tuījìn Wǎngluò Ānquán Zhànlüè Jiànshè = [Exploring a

New Model for Strategic Mutual Trust and Cross-Border Data Flow Management: Promoting Cybersecurity Strategy Construction with "Data Sovereignty" as the Core]. **Xìnxī Ānquán yǔ Tōngxìn Bǎomì** = [**Information Security and Communications Privacy**], [China], n. 12, p. 13-16, 2018.

SUN, Xiaoyue. Duōwéi Xiétóng Shìyù Xià Xūjiǎ Xìnxī Chuánbò de Zhìlǐ Lùjìng = [Governance Pathways for Disinformation Dissemination from a Multidimensional Collaborative Perspective]. **Zhōngguó Dìshì Bào Rén** = [**China City Newspaper**], [China], n. 1, p. 85-87, 2025. DOI: 10.16763/j.cnki.1007-4643.2025.01.009. Acesso em: 24 fev. 2025.

UNITED NATIONS. **UN Global Principles for Information Integrity**. New York: United Nations, 2024a. Disponível em: https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf. Acesso em: 24 fev. 2025.

UNITED NATIONS. **World Population Prospects 2024**. New York: United Nations, 2024b. Disponível em: https://population.un.org/wpp/. Acesso em: 24 fev. 2025.

VON SOLMS, Rossouw; VAN NIEKERK, Johan. From information security to cybersecurity. **Computers & Security**, [United States], v. 38, p. 97-102, out. 2013. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801. Acesso em: 24 fev. 2025.

WANG, Richard; STRONG, Diane. Beyond accuracy: What data quality means to data consumers. **Journal of Management Information Systems**, [*s. l.*], v. 12, n. 4, p. 5-33, 1996. Disponível em: http://mitiq.mit.edu/Documents/Publications/TDQMpub/14_Beyond_Accuracy.pdf. Acesso em: 24 fev. 2025.

WORLD BANK. **GDP** (current US$). [*S. l.*], 2023. Disponível em: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD. Acesso em: 24 fev. 2025.

WORLD ECONOMIC FORUM. **The Global Risks Report 2023**. [*S. l.*], 2023. Disponível em: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf. Acesso em: 24 fev. 2025.

XI, Jinping. Xi Jinping zai dier jie shijie hulianwang dahui kaimushi shang de jianghua = [Xi Jinping's speech at the opening ceremony of the 2nd World Internet Conference.]. **Xinhua News**, [*s. l.*], 2015. Disponível em: https://www.gov.cn/xinwen/2015-12/16/content_5024712.htm. Acesso em: 24 fev. 2025.

XIONG, Guangqing; WANG, Rui. Quánqiú hùliánwǎng zhìlǐ zhōng de wǎngluò zhǔquán: Lìshǐ yǎnjìn, guójì zhēngyì hé zhōngguó lìchǎng = [Cyber Sovereignty in Global Internet Governance: Historical Evolution, International Disputes, and China's Position]. **Xuéxí yǔ tànsuǒ** = [**Study & Exploration**], [China], n. 4, p. 24-176, 2024.

YUAN, Sha. Zǒngtǐ Guójiā Ānquán Guān Shìyù Xià de Xūjiǎ Xìnxī Yánjiū = [Research on Disinformation from the Perspective of Holistic National Security]. **Guójì Ānquán Yánjiū** = [**Journal of International Security Studies**], [China], v. 40, n. 3, p. 32-56, 157-158, 2022. DOI: 10.14093/j.cnki.cn10-1132/d.2022.03.002. Acesso em: 24 fev. 2025.

ZHAI, Zhiyong. Shùjù Zhǔquán de Xīngqǐ jí Qí Shuāngchóng Shǔxìng = [The Rise of Data Sovereignty and Its Dual Attributes]. **Zhōngguó Fǎlǜ Pínglùn** = [**China Law Review**], [China], n. 6, p. 196-202, 2018.

ZHANG, Chao; DUAN, Weiyu; CHEN, Kaihua; YANG, Xiaoguang; LONG, Yuntao. Xìnxī Jìshù Tuījìn Guójiā Zhìlǐ Xiàndàihuà de Zhànlüè Yánjiū - Dì S70 Cì Xiāngshān Kēxué Huìyì Xuéshù Zòngshù = [Strategic Research on Information Technology Promoting the Modernization of National Governance: An Academic Summary of the 70th Xiangshan Science Conference]. **Zhōngguó Kēxuéyuàn Yuànkān** = [**Bulletin of the Chinese Academy of Sciences**], [Beijing, China], v. 39, n. 1, p. 143-151, 2024. DOI: 10.16418/j.issn.1000-3045.20231219003. Acesso em: 24 fev. 2025.