

ARTICLE

The Problems of Information Sovereignty in the BRICS Countries

Elena L. Andreeva,

Institute of Economics of the Ural Branch of Russian Academy of Science
(Yekaterinburg, Russian Federation)

<https://orcid.org/0000-0003-4975-0905>

<https://doi.org/10.21684/2412-2343-2026-13-1-76-88>

Received: March 23, 2025

Reviewed: May 20, 2025

Accepted: November 26, 2025

Abstract. This article illustrates the nature and significance of information sovereignty in the expanding BRICS regions. The study adopts an approach that considers sovereignty as an integral system of political and legal relations, institutions, and values. Its main components include technological and ideological elements. In the context of growing global information challenges and threats, it is necessary to implement a targeted state policy to ensure information sovereignty for BRICS member states and their joint efforts to defend the interests of the global majority. To ensure information sovereignty, it is necessary to combine the tools of the so-called “information shield” and “information sword” in the information policy. BRICS serves as a communication platform that facilitates the effective exchange of best practices. As an expanded format, BRICS can make greater use of the advantages of “soft power,” which affirms the legitimacy of decisions by garnering the support of representatives of developing countries. BRICS has significant potential in the field of coordination and the formation of common principles and approaches to the implementation of information sovereignty. It also allows for the expansion of a common approach by involving developing countries in cooperation and extending the norms and rules of information sovereignty to the countries of the global majority.

Keywords: information sovereignty; information policy; digital economy; BRICS; global information space.

To cite: Andreeva, E. L. (2026). The problems of information sovereignty in the BRICS countries. *BRICS Law Journal*, 13(1), 76–88.

Table of Contents

Introduction

1. Concept of Information Sovereignty in World Economic Situations

2. Approaches to the Formation of Information Sovereignty in Developed and Developing Countries

3. Information Sovereignty of the BRICS Countries: Strengths and Weaknesses

4. Prospects of Information Policy in the BRICS Alliance

Conclusion

Introduction

In recent years, the issue of sovereignty has gained increasing relevance both in legal and economic discourse, including within socioeconomic spheres. The problem of information sovereignty has attracted particular attention due to the rapid development of the digital economy, both at the level of individual countries and in the global economy as a whole. In the context of the ongoing global economic transformations, the BRICS alliance is one of the promising integration entities, attracting a growing number of countries interested in interacting under new, flexible, or so-called “soft” conditions. This expansion makes it especially relevant to examine issues related to a common understanding of the nature and meaning of information sovereignty in the expanding BRICS countries.

1. Concept of Information Sovereignty in World Economic Situations

Traditionally, it is believed that the concept of “sovereignty” was introduced in the 14th century by the French thinker J. Bodin in his work *Six Books on the State* (1576). It was connected with the historical conditions and justified the unshakable power of the monarch (in other words, the “sovereign”) over a certain territory, which was necessary at that time. Long before even J. Bodin, the discussion concerning the subject having the right to absolute power (the Almighty or the Church in the person

of the Pope) had been conducted many times. The main criterion of this discussion was related to the principles of justice and value systems.

Methodologically, it is important to consider the concept of “sovereignty” both in relation to the new sphere of information and to the new object, such as the integration of countries representing the interests of the participating countries. These interests are often easier to defend through joint efforts. In the context of digitalization, however, it is harder to connect the international economic organizations to a specific territory because we are often talking about a virtual information space.

Sovereignty is a holistic system of political and legal relations, institutions, and values that constitute the core of society, including ideological, moral and interpersonal relations. It is a set of concepts, relations, norms, and instruments of influence that represent the category of both state and international law and characterize relations between entities of different levels.

When speaking about the traditional concept of “sovereignty,” in foreign policy it refers to “the independence and equality of the state as a subject of international law in relations with other states, ensuring the equality of all states in the sphere of international relations.” According to A.A. Efremov,¹ information sovereignty can be understood as the supremacy and independence of state power in the formation and implementation of information policy in the national segment and the global information space. This definition makes it clear that both national and global segments play an important role in its regulation.

A.V. Rossoshansky² connects information sovereignty with the ability and intention of any subject of politics (including integration associations) to carry out information activities across the full cycle of production, in all its components: production, distribution, and consumption of information, guided, primarily, by its own interests of participation in politics, and using “information as a resource of political influence on a scale and volume corresponding to current and long-term interests.” In this context, it is crucial to define both current and long-term interests and priorities, as well as to link them to relevant strategies, mechanisms, and tools for developing information policies and thus building information sovereignty.

Regarding BRICS, an active information policy can be observed, especially on the eve of the 2024 Summit in Kazan, which resonated with the decisions taken by the countries to join the organization in various capacities, including as observers. An active information policy has also been demonstrated by Western countries, which have closely monitored this process and have made efforts to counter the successes of the BRICS development.

¹ Efremov, A. A. (2017). Formation of the concept of state information sovereignty. *Law. Journal of the Higher School of Economics*, 1, 201–215. (In Russian).

² Rossoshansky, A. V. (2011). Political and informational sovereignty in context of globalization processes. *Simbirsk Scientific Journal Vestnik*, 4(6), 176–186. (In Russian).

As M.M. Kucheryavyy & Yu.V. Vovenda³ note, information policy is implemented in the information-technological, information-psychological, and information-political spheres. Information sovereignty consists of digital, mental, and power sovereignty. Digital sovereignty is determined by the appropriate level of technology. It requires the existence of a full cycle of domestic production of equipment and software, including domestic search engines, a national segment of the Internet and social networks, as well as information security tools and a national payment system. Mental sovereignty is related to the level of education and information culture in general, as well as the presence of a suitable unifying idea or ideology. Power sovereignty depends on the information policy pursued, the level of public trust, the patriotism of the managerial elite, the media, and the stability and sustainability of the national currency.⁴

Moreover, if these functions are not provided by the state or the integration association, they will be controlled by other foreign representatives who will defend their interests to the detriment of the country's economy or transforming it into a mere raw material appendage. Therefore, ideological sovereignty, determined by the presence of one's own ideology and culture, plays a special role in the formation of information sovereignty. If this element does not exist, an alien culture can be imposed on society, leading to losing the state itself. The Russian Federation's Information Security Doctrine states, "The interests of the state in the information sphere are to create conditions for ensuring the sovereignty and territorial integrity of Russia."⁵

The creation of these conditions is influenced by both internal and external challenges and threats. Internal threats include lagging behind the leading Western countries in the level and pace of information technology, underdeveloped domestic production, an incomplete regulatory framework, etc. External threats include the waging of an information war by the countries of the collective West, violations of Russia's national interests and attempts to push it out of the information and communications technology market, and the development of concepts of information confrontation by Western countries.

In this regard, it is necessary to implement a targeted state policy of information sovereignty formation in the following main areas to overcome these threats:

- defining the geopolitical information interests of the country, including common interests with other countries, especially with BRICS;
- advocating for and protecting the formation of a regulatory framework and norms of international law at the international level in the interests of ensuring the information sovereignty of friendly countries and their integration entities;

³ Kucheryavyy, M. M., & Vovenda, Yu. V. (2016). Regional information security within the framework of the Eurasian integration. *Administrative Consulting*, 7, 19–26. (In Russian).

⁴ Kucheryavyy, M. M. (2015). Awareness information sovereignty in the trends of global information space. *Science, New Technologies and Innovations in Kyrgyzstan*, 12, 22–27. (In Russian).

⁵ President of the Russian Federation. (2000, September 9). *Doctrine of information security of the Russian Federation* (Decree No. Pr-1895). Rossiiskaia Gazeta. http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm. (In Russian).

- creating common protected information networks and systems that ensure secure interaction with the global information space, or establishing common rules and instruments that limit such interaction in the national interests of countries;
- conducting active international diplomatic, cultural, and educational activities to strengthen the information sovereignty of the countries of the BRICS integration association and to promote the formation of their positive image at the international level.

2. Approaches to the Formation of Information Sovereignty in Developed and Developing Countries

The category of “independence” in international relations has its own peculiarities. States are “bound” by the principles enshrined in the UN Charter, international treaties, and participation in international organizations. The freedom of cross-border information flows is implemented by the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966).

The term “cyberspace” is actively used in international legal documents, such as the Okinawa Charter on the Global Information Society (2000) and the Convention on Cybercrime (2001). The report of the Group of Governmental Experts to the 68th session of the UN General Assembly (2013) states that state sovereignty and international norms and principles derived from the principle of state sovereignty extend to the conduct of states in the context of activities related to the use of ICT. It also addresses the jurisdiction of states over the ICT infrastructure on their territory (para. 20).

A similar position is included in the report of the Group of Governmental Experts of the 70th session of the General Assembly (2015). It should be noted that the growing importance of information sovereignty as a tool of the state to influence the flow of information in the country is characteristic of countries that claim leading positions in the development of information technologies (the US, China, South Korea, South Africa, UAE, Iran, Russia, etc.). In the early 2000s, M. Price’s⁶ monograph *Media and Sovereignty* was one of the most cited abroad. The Chinese professor W. Gong⁷ considered information sovereignty through its internal and external components.

However, if developing countries see a threat to their sovereignty in the unlimited flow of information, developed countries, on the contrary, consider the free dissemination of information as a factor of strengthening their sovereignty.⁸ The emergence of

⁶ Price, M. E. (2002). *Media and sovereignty: The global information revolution and its challenge to state power* (p. 352). MIT Press.

⁷ Gong, W. (2005). Information sovereignty reviewed. *Intercultural Communication Studies*, 14(1), 119–135.

⁸ Damon, L. (1986). Freedom of information versus national sovereignty: The need for a new global forum for the resolution of transborder data flow problems. *Fordham International Law Journal*, 10(2), 262–287.

works analyzing the Internet itself as a threat to state sovereignty can be noted.⁹ At the same time, in Western science, such a concept is considered exclusively critical, as characteristic of authoritarian regimes, and, therefore, primarily pursues its own interests in gaining leading positions in this area. Representatives of developing countries stress the importance of respecting the cultural sovereignty of each country, while traditional “information” leaders are interested in complete freedom of information flow.¹⁰

The legal aspects of state sovereignty in the information sphere in Russia were first noted by V.B. Naumov¹¹ in 1999, based on the analysis of the first court cases related to the cross-border dissemination of information via the Internet. The judicial approach to Internet regulation is also reflected in the works of I.Yu. Bogdanovskaya.¹² The relationship between sovereignty and jurisdiction is revealed in the works of L.V. Terentieva.¹³ In the doctrine of international law, the relationship between sovereignty, territorial supremacy and jurisdiction is reduced to the following formula: jurisdiction is one of the elements of the territorial supremacy of the state, which in turn is an integral part of its sovereignty.¹⁴ The adoption of federal laws in the Russian Federation, including the Federal Law of July 26, 2017 “On the Security of the Critical Information Infrastructure of the Russian Federation,” is more connected with the desire to “protect sovereignty” than with the development of a conceptual basis for its active formation. In this context, it is necessary to distinguish between national critical infrastructure,¹⁵ which encompasses defense systems, banking and financial systems, telecommunications systems, energy systems, etc., and critical information infrastructure, which includes telephone exchanges, Internet traffic exchanges, wireless networks, satellites, etc.¹⁶

The concept of data sovereignty gained widespread recognition with the adoption of legislation in the EU and individual countries, including Russia, which

⁹ Perrit, J. (1998). The internet as a threat to sovereignty? Thoughts on the internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies*, 5(2), 423–442.

¹⁰ Drake, W. J., & Price, M. E. (2014). *Beyond NETmundial: The roadmap for institutional improvements to the Global Internet Governance Ecosystem*. University of Pennsylvania.

¹¹ President of the Russian Federation, 2000.

¹² Bogdanovskaya, I. Yu. (2001). The Internet: Global regulation and national jurisdictions. *Scientific and Technical Information Processing. Series*, 1(10), 1–3. (In Russian).

¹³ Terentieva, L. V. (2010). Cyberspace and state borders: Jurisdictional issues on the Internet. *Law. Journal of the Higher School of Economics*, 1, 63–68. (In Russian).

¹⁴ Kayumova, A. R. (2008). Sovereignty and state jurisdiction: Problems of correlation. *Constitutional and Municipal Law*, 9, 12–15. (In Russian).

¹⁵ <https://www.itu.int/itu-d/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf>

¹⁶ Brunner, E. M., & Suter, M. (Eds.). (2009). *International CIIP handbook 2008/2009: An inventory of 25 national and 7 international critical information infrastructure protection policies*. Center for Security Studies, ETH Zurich. css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf

provides for the mandatory processing of citizens' personal data on servers in a given state and subordination to the jurisdiction of the country where this information is located.¹⁷ These requirements are aimed at protecting the interests of nation states in relation to the confidentiality and integrity of data.¹⁸

Among the documents in the framework of integration associations, several key strategic documents can be highlighted. These include the EU Digital Single Market (DSM) strategy adopted in 2015; the OECD Cancun Declaration of the Organisation for Economic Cooperation and Development of the Digital Economy: "Innovation, growth and social well-being" adopted in 2016, and the "Digital Agenda of the Eurasian Economic Union" adopted in the EAEU on October 27, 2016.^{19/20}

A noteworthy approach is presented in the works of E.G. Zorina²¹ and I.S. Ashmanov,²² Who emphasize that the state in its information policy must competently combine the methods of the "information shield" and the "information sword." I.S. Ashmanov describes the "information shield" as a set of protective technical, communication, ideological, and cultural means used to neutralize information that is unprofitable for the state, to counter attempts to steal strategically important information, and to protect the national payment system. In his view, the "information sword" is a set of offensive methods and actions that are aimed at undermining the information sovereignty of the enemy. Thus, an "information shield" refers to passive elements and defensive measures, while an "information sword" refers to offensive and active tools. In order to ensure information sovereignty, it is necessary to combine the tools of the "information shield" and the "information sword" in information policy.

In this conceptual framework, the main elements of the "shield" are a high level of computerization of the state and its provision with communication systems, its own software and national data protection systems, as well as a positive internal and external image of the state and an idea or ideology, in the absence of which foreign,

¹⁷ De Filippi, P., & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, 3(2). <http://ssrn.com/abstract=2167372>

¹⁸ Nugraha, Y., & Sastrosubroto, K. (2015). Towards data sovereignty in cyberspace. In *Proceedings of the 3rd International Conference on Information and Communication Technology, Nusa Dua, Indonesia, May 27–29, 2015* (pp. 465–471).

¹⁹ <http://www.eurasiancommission.org/ru/act/dmi/SiteAssets/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9%D0%B4%D0%B5%D0%BA%D0%BB%D0%B0%D1%80%D0%B0%D-1%86%D0%B8%D0%B8%20v%2011.pdf>.

²⁰ Eurasian Economic Commission. (n.d.). *The EAEU's digital agenda was discussed for the first time in Kazakhstan*. <http://www.eurasiancommission.org/ru/nae/news/Pages/01-06-2016-4.aspx>

²¹ Zorina, E. G. (2017). Information sovereignty of the modern state and the main instruments for ensuring it. *Izvestiya of Saratov University. New Series. Series: Sociology. Political Science*, 17(3), 345–348. (In Russian).

²² Ashmanov, I. S. (n.d.). *Information sovereignty*. <http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf>. (In Russian).

including destructive, ideas penetrate the ideological field. The offensive elements of the “sword” include a developed system of media and propaganda, the production and popularization of national cultural products, values, and ideas among internal and external audiences, including through the Internet and mass culture.

Thus, the concept of “information sovereignty” presupposes a well-considered combination of the two most important aspects: technological and ideological. If the first includes the presence of national software, its own social networks, search engines, and a national electronic payment system, then the second includes the presence of an official ideology or idea, a high level of information culture, a developed propaganda system, as well as relevant legislation in the field of information.

3. Information Sovereignty of the BRICS Countries: Strengths and Weaknesses

For objective reasons related, on one hand, to the dynamics of the development of digital relations in all spheres of life and, on the other, to the proportional increase of threats and risks to information sovereignty, information cooperation has become one of the most popular areas of interaction within the BRICS countries.²³ The principal areas for the implementation of state sovereignty in the information sphere are the formation of international legal regulation of the information space on the basis of the principle of sovereign equality of all states, as well as the formation of information policy within the common information space of the BRICS countries.

Partnership within the BRICS framework is built on the basis of the UN Charter, principles, and norms of international law, as well as the principles agreed upon at the III BRICS summit in Sanya (China) on April 13–14, 2011.²⁴ The principles specified in the acts include openness, pragmatism, solidarity, non-bloc character, and non-direction against third parties.

These issues were also reflected in the eThekwini (2013)²⁵ and Fortaleza (2014) Declarations,²⁶ which served as the basis for consolidating the efforts of BRICS member states to address digital challenges through the establishment of the BRICS Working Group on Security in the Use of Information and Communication Technologies in

²³ Lazanyuk, I. V., Shkvarya, L. V., & Eeberdyeva, M. M. (2025). Development of AI in the BRICS countries: Synergy to reduce digital inequality. *Vostok (Oriens)*, 1, 182–194. (In Russian).

²⁴ President of the Russian Federation. (2011, April 14). *Declaration adopted following the BRICS Summit in Sanya*. Official website of the President of the Russian Federation. <http://kremlin.ru/supplement/907>. (In Russian).

²⁵ President of the Russian Federation. (2013, March 27). *Ethekwini Declaration and Ethekwini Action Plan*. Official website of the President of the Russian Federation. <http://kremlin.ru/supplement/1430>. (In Russian).

²⁶ President of the Russian Federation. (2014, July 15). *Fortaleza Declaration*. Official website of the President of the Russian Federation. <http://static.kremlin.ru/media/events/files/41d4f1dd6741763252a8.pdf>. (In Russian).

2014.²⁷ In 2016, the BRICS Joint Action Plan on ICT was adopted. Earlier, in 2015, the first meeting of BRICS communications ministers announced the need for a unified approach to developing digital sovereignty principles.²⁸

To characterize BRICS' technological sophistication, we can use the methodology of the International Telecommunication Union, the United Nation's leading ICT agency, which promotes global communications and covers three main sectors: radio communications (ITU-R), standardization (ITU-T), and development (ITU-D). According to their estimates, the BRICS countries can be roughly divided into three groups in terms of their participation in international processes of information security development: "leading" countries with a complex ICT system, "intermediate" countries with dynamically developing infrastructures, and "developing" countries where progress is concentrated in individual areas of development.²⁹

The first group includes Russia, India, Saudi Arabia, and the UAE. At the same time, while Russia and India are characterized by gradual advancement, Saudi Arabia and the UAE are focused on the accelerated achievement of leading positions in the global digital space.

The second group, according to this methodology, includes China, Brazil, and Egypt. Some doubts may arise regarding the inclusion of China in this group, given its status as a technological leader. However, this classification can be explained by the specific features of China's regulation of the Internet space, which limit the participation of the private sector in the development of international projects in the information field. In addition, the PRC has recently been actively disseminating its experience in managing the digital space, notably through the "Digital Silk Road" initiative. This approach contributes, on one hand, to strengthening China's international technological position and, on the other hand, to reinforcing its information sovereignty.

The third group includes Iran and South Africa. Despite Iran's significant achievements in the high-tech sector, its international cooperation is affected by its confrontation with both Western and regional partners (most notably Israel and the UAE). In this respect, BRICS can play the role of a communication platform where an effective exchange of best practices is possible without the risk of aggravating some bilateral relations (China–India, Saudi–Iran, and the UAE–Iran). At the same time, it seems that the BRICS countries should focus less on the existing differences and more on their shared common interests. For example, the head of the BRICS Research Centre at Fudan University, Shen Yi, notes that the main threat to the BRICS countries

²⁷ Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (2016, November 11). *Joint action plan of BRICS countries in the field of information and communication technologies adopted*. <https://digital.gov.ru/ru/events/36049/>. (In Russian).

²⁸ Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (2015, October 22). *The first-ever meeting of ICT ministers of BRICS countries launched*. <https://digital.gov.ru/ru/events/34185/> (In Russian).

²⁹ Ignatov, A. A., & Zinovieva E. S. (2024, January 24). *Digital sovereignty in the BRICS agenda*. Russian International Affairs Council. (In Russian).

in cyberspace comes from the United States, because Washington seeks to secure its own geopolitical interests at the expense of the sovereignty of other actors.³⁰

Despite the differences in the level of digital development of BRICS countries, Russia and China are actively strengthening their presence in the digital space. Infrastructural cooperation has been particularly consolidated by China, which has initiated numerous infrastructure projects to strengthen its position as a leading center of power in the digital space. These efforts are embedded within the broader framework of the formation of a “community of common destiny in cyberspace,” which emphasizes respect for information sovereignty. In this context, in 2016, China adopted the Cybersecurity Law and the National Cyberspace Security Strategy.

In September 2020, China presented the Global Data Security Initiative, which emphasizes the importance of respecting state sovereignty in the field of data, as well as the central role of the United Nation in international cooperation. Russia supported China’s vision. The issue of information security has also been elevated on the BRICS agenda through the efforts of Russia, which initiated the discussion of this issue at the global level.

In 2018, Russia initiated the creation of an Open-Ended Working Group (OEWG).³¹ The OEWG aims to involve all UN member states in the discussion of rules and principles of responsible state behavior in the field of ICT. The United States proposed a competing format to the Russian project—a group of governmental experts composed of 15 to 25 states. In November 2023, within the framework of the vote in the UN General Assembly, both the Russian and US draft resolutions were adopted. The Russian proposal, co-authored by China and Iran, was supported by all BRICS countries, while the US proposal was not supported by Russia, China, and Iran.

The importance of information security is also reflected in the Foreign Policy Concept of the Russian Federation, approved by the President of the Russian Federation Vladimir Putin on March 31, which states that the Russian Federation intends to pay priority attention to “strengthening and improving the international legal regime regulating activities in the global information space.” India is also close to Russia and China in terms of legislative activity in this area. Together, these three BRICS countries claim the role of power centers in the global information space. With the entry of Saudi Arabia, the United Arab Emirates, and Iran into the BRICS, further cooperation in this field can be expected. For example, at the end of April 2024, the international technology company GDA Group, within the framework of a forum in the UAE, proposed an initiative to create a BRICS convention on secure artificial intelligence. Similar ideas were expressed within the framework of the Dubai

³⁰ TASS. (2024, April 10). *Expert says the biggest digital threat to BRICS countries comes from the USA*. <https://tass.ru/mezhdunarodnaya-panorama/20503645>

³¹ Tolstukhina, A. V. (2019, February 13). *Better two cyber resolutions than none*. Russian International Affairs Council. (In Russian). <https://russiancouncil.ru/analytics-and-comments/analytics/luchshe-dve-kiberrezolyutsii-chem-ni-odnoy/>

FinTech Summit in May 2024, confirming the interest of the participating countries in coordinating joint efforts within the framework of the BRICS alliance.³²

4. Prospects of Information Policy in the BRICS Alliance

The BRICS expansion brings significant image-related benefits.³³ The inclusion of an increasing number of developing countries strengthens the image of BRICS as an association representing the interests of the global South or the global majority. In an expanded format, BRICS can make greater use of the advantages of soft power.³⁴ This ensures multilateral coordination and enhances the legitimacy of decisions by winning over representatives of the developing world. In the future, it is necessary to develop priorities in order to achieve a positive effect of international cooperation in these areas. These include the development of human and intellectual potential of the BRICS countries, the industrial production of final products of innovation and technologies, the promotion of basic research and development, etc.³⁵

Special attention should be paid to coordination of scientific cooperation. The BRICS Steering Committee for Science, Technology, and Innovation was established by the BRICS countries in 2019 at the initiative of Russia. This committee combines the coordination functions at the level of individual BRICS member countries, which are performed by the Institute of Applied Economic Research in Brazil, the Observer Research Foundation in India, the Chinese Council of BRICS Research Centers in China, the South African BRICS Research Center in South Africa, and the National BRICS Research Committee (NCI BRICS) in Russia. The National Committee for BRICS Research in Russia was established in 2011 by the Russian Academy of Sciences and the Russkiy Mir Foundation.

The BRICS countries provide each other with access to scientific infrastructure facilities within the framework of the Global Network of Advanced Research Infrastructures BRICS GRAIN. This platform was created on the initiative of Russia, which provides scientists from the BRICS countries with access to mega science projects. Russia and India each provided six infrastructure facilities, Brazil and China each provided four facilities, and South Africa provided one.³⁶ A further seven

³² Zinovieva E., & Yacze B. (2019, February 13). *Better two cyber resolutions than none*. Russian International Affairs Council. (In Russian). <https://russiancouncil.ru/analytics-and-comments/analytics/luchshe-dve-kiberrezolyutsii-chem-ni-odnoy/>

³³ Pupkova, A. (n.d.). *International image of a country: Theoretical aspects*. Politicheskoe obrazovanie. <http://lawinrussia.ru/content/mezhdunarodnyy-imidzh-strany-teoreticheskie-aspekty>. (In Russian).

³⁴ Gavra, D. P., Savitskaya, A. S., & Shishkin, D. P. (2011). External image of the state in the media space. *Vestnik of Saint Petersburg State University*, 9(3), 187–196. (In Russian).

³⁵ Olejnik, G. V. (2023). BRICS national interests in the field of scientific and technological cooperation. *Russian Foreign Economic Bulletin*, 3, 29–40. (In Russian).

³⁶ Toloraya, G. D., et al. (2023). *Promising directions of scientific cooperation: BRICS countries* (Report No. 90). Russian International Affairs Council. (In Russian).

facilities are under development, one each in South Africa, India, and Brazil, and four in Russia. Through the development of shared research facilities and coordinated innovation, this platform contributes to the development of international scientific and technological cooperation, including in the field of ICT. This, in turn, contributes to the development of information sovereignty of the BRICS countries and the creation of a positive image of the countries in the global information space.

Conclusion

Thus, BRICS possesses significant potential in the field of coordination and the formation of common principles and approaches to the implementation of information sovereignty at the United Nations level. In the current conditions of escalating international competition for new instruments of global influence, such as global norms and institutions and technological standards, the BRICS framework allows for the expansion of a common approach by involving developing countries in cooperation and extending the norms and rules of information sovereignty to the countries of the global majority.

Russia and China, as well as other BRICS partner countries, offer an alternative vision of the global information sphere based on respect for state sovereignty. Enhanced interaction and exchange in the development of information technologies within the framework of BRICS cooperation in the fields of science, education, and culture will enable BRICS to increase its role and significance in the global economy and improve living standards in developing countries.

References

Damon, L. (1986). Freedom of information versus national sovereignty: The need for a new global forum for the resolution of transborder data flow problems. *Fordham International Law Journal*, 10(2), 262–287.

De Filippi, P., & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, 3(2). <http://ssrn.com/abstract=2167372>

Drake, W. J., & Price, M. E. (2014). *Beyond NETmundial: The roadmap for institutional improvements to the Global Internet Governance Ecosystem*. University of Pennsylvania. <https://doi.org/10.5167/uzh-99003>

Efremov, A. A. (2017). Formation of the concept of state information sovereignty. *Law. Journal of the Higher School of Economics*, 1, 201–215. <https://doi.org/10.17323/2072-8166.2017.1.201.215>. (In Russian).

Gavra, D. P., Savitskaya, A. S., & Shishkin, D. P. (2011). External image of the state in the media space. *Vestnik of Saint Petersburg State University*, 9(3), 187–196. (In Russian).

Gong, W. (2005). Information sovereignty reviewed. *Intercultural Communication Studies*, 14(1), 119–135.

Kucheryavyy, M. M., & Vovenda, Yu. V. (2016). Regional information security within the framework of the Eurasian integration. *Administrative Consulting*, 7, 19–26. (In Russian).

Lazanyuk, I. V., Shkvarya, L. V., & Eeberdyeva, M. M. (2025). Development of AI in the BRICS countries: Synergy to reduce digital inequality. *Vostok (Oriens)*, 1, 182–194. <https://doi.org/10.31696/s086919080033712-0>. (In Russian).

Olejnik, G. V. (2023). BRICS national interests in the field of scientific and technological cooperation. *Russian Foreign Economic Bulletin*, 3, 29–40. (In Russian).

Perrit, J. (1998). The internet as a threat to sovereignty? Thoughts on the internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies*, 5(2), 423–442.

Price, M. E. (2002). *Media and sovereignty: The global information revolution and its challenge to state power*. MIT Press. <https://doi.org/10.7551/mitpress/4533.001.0001>

Rossoshansky, A. V. (2011). Political and informational sovereignty in context of globalization processes. *Simbirsk Scientific Journal Vestnik*, 4(6), 176–186. (In Russian).

Terentieva, L. V. (2010). Cyberspace and state borders: Jurisdictional issues on the Internet. *Law. Journal of the Higher School of Economics*, 1, 63–68. (In Russian).

Toloraya, G. D., et al. (2023). *Promising directions of scientific cooperation: BRICS countries* (Report No. 90). Russian International Affairs Council. (In Russian).

Zorina, E. G. (2017). Information sovereignty of the modern state and the main instruments for ensuring it. *Izvestiya of Saratov University. New Series. Series: Sociology. Political Science*, 17(3), 345–348. <https://doi.org/10.18500/1818-9601-2017-17-3-345-348>. (In Russian).

Information about the author

Elena L. Andreeva (Yekaterinburg, Russia) – Professor, Head, Centre of Regional Comparative Research, Institute of Economics, Ural Branch of Russian Academy of Science (29 Moskovskaya St., Yekaterinburg, 620014, Russian Federation; e-mail: andreeva.el@uiec.ru).