Russian Journal of World Politics and Law of Nations. 2024. 3(1). P. 54–82
DOI 10.24833/RJWPLN-2024-1-54-82 Research Article

The Role of Brics in The International ICT Security Regime[1]

Elena S. Zinovieva[1], Alexander A. Ignatov[2]

[1] MGIMO University
[2] MGIMO University, Russian Presidential Academy of National Economy and Public Administration

Abstract. The ubiquitous implementation of information and communication technologies (ICTs) is giving rise to cross-border security threats that require joint international responses. Fragmentation and growing conflict in the global information space complicate international cooperation within the UN to form a comprehensive global information security regime. Western countries actively support the formation of a cyber security regime based on Western values and promoted as a general initiative of the international community, without taking the position of developing countries into account. An alternative approach focused on securing digital sovereignty is being promoted by many non-Western negotiating platforms, among which the BRICS occupies an important place. This article aims to assess the potential of the BRICS influence on the international ICT security regime and the main directions of the association's activities in this area. In this paper, the BRICS ICT security agenda is studied on the basis of official documents of the association's annual summits and the main commitments made by the member countries. The discourse analysis of the strategic planning documents of the BRICS countries allows to identify their priorities in this area, and to assess the potential for the implementation of these obligations at the BRICS level. All the BRICS countries focus on ensuring ICT sovereignty. However, Russia, India, and China consider digital development and ICT security as the most important area of state policy and international cooperation. They are also more advanced when it comes to digital technologies compared to the other BRICS countries, which means they are more vulnerable. In turn, Brazil and South Africa do not consider this area as a priority, placing greater emphasis on ICT development, access to technology, and bridging the digital divide. However, all five countries are interested in solving the problem of extremism and terrorism in the digital sphere, which is also a promising area for BRICS multilateral cooperation. A study of the voting of the BRICS countries in the UN and an analysis of their participation in alternative initiatives in the formation of a cyber security regime promoted by Western countries showed the high efficiency of BRICS as a negotiating platform. Its main contribution in this respect is the development of a common position on the norms and principles of the international information security regime and their support at the UN level. Thus, BRICS can make a constructive contribution to the formation of the norms and principles of the international ICT security regime based on the principles of respect for state sovereignty, the internationalization of internet gov-

[1] English translation from the Russian text: Zinovieva E. S., Ignatov A.A. 2023. BRIKS v global'nom rezhime IKT-bezopasnosti. *Mezhdunarodnye protsessy* [International Trends]. 21(4). P. 104–132. DOI: 10.17994/IT.2022.20.3.70.4

ernance, and combatting to the criminal use of ICTs. An important advantage of BRICS in this area is the possibility of aggregating the interests and positions of developing countries.

Keywords: BRICS; discourse analysis; ICT security; digital economy; global governance

Digital technologies, and the internet in particular, have penetrated all spheres of society. As the infrastructural basis of the growing digital economy (Bukht, Hiks 2018), the internet is also a source of threats to the security of the individual and the state (Krutskikh 2007; Krutskikh, Streltsov 2014; Bezkorovajnyj, Tatuzov 2014; Zgoba et al 2014; Karpova 2014; Malakhin, Malakhina 2018; Romashkina 2020).

The importance of combatting information threats has been written into both the National Security Strategy of the Russian Federation and the Doctrine of Information Security of the Russian Federation.[2] It also appears in similar documents of leading international players concerning the development of the digital economy.[3] Specifically, Russia's partners in BRICS (Brazil, India, China, and South Africa) have adopted documents enshrining the importance of ICT security issues at the national and global levels.[4]

A significant topic on the international agenda is the development of rules for regulating and ensuring the safe development of the ICT space. This issue is being addressed by the United Nations,[5] but in the 2020s, the United States and its allies have put forward a number of initiatives aimed at creating alternative regimes outside of the UN system, including the Paris Call for Trust and Security in Cyberspace,[6]

---

[2] Decree No. 400 of the President of the Russian Federation "On the National Security Strategy of the Russian Federation" of July 2, 2021. URL: http://www.kremlin.ru/acts/bank/47046 (accessed: 11.09.2022); Decree No. 646 of the President of the Russian Federation "On Approving the Doctrine of Information Security of the Russian Federation" of December 5, 2016. URL: http://kremlin.ru/acts/bank/41460 (accessed: 11.09.2022).

[3] See: The EU's Cybersecurity Strategy for the Digital Decade. 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (accessed: 4.08.2022); White House Interim National Security Strategic Guidance. 2021. URL: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf (accessed: 27.01.2022).

[4] See: National Information Security Policy of Brazil. 2019. URL: https://www.gov.br/governodigital/pt-br/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao (accessed: 11.09.2022); National Digital Communications Policy India. 2018. URL: https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf (accessed: 11.09.2022); India's National Security Strategy. 2019. URL: https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf (accessed: 11.09.2022); The National Cybersecurity Policy Framework South Africa. 2019. URL: https:// www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed: 11.09.2022); International Strategy of Cooperation on Cyberspace China. 2017. URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html#:~:text=The%20strategic%20goal%20of%20China's,peace%2C%20security%20and%20stability%20in (accessed: 11.09.2022); Global Initiative on Data Security. 2020. URL: https://www.fmprc.gov.cn/mf (accessed: 11.09.2022).

[5] See: Report A/68/98 of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security dated June 24, 2013. URL: https://namib.online/wp-content/uploads/2020/04/Report-of-the-UN-Group-of-Governmental-Experts-on-Developments-in-the-Field-of-Information-of-24-June-2013.pdf (accessed: 11.09.2022); Resolution GA73/27 "Developments in the field of information and telecommunications in the context of international security" of December 5, 2018. URL: https://namib.online/wp-content/uploads/2020/04/Developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-UN-GA-Resolution-A7327-on-5-December-2018.pdf (accessed: 11.09.2022) and others.

[6] Paris Call for Trust and Security in Cyberspace. URL: https://pariscall.international/en/call (accessed: 11.09.2022).

and the Declaration for the Future of the Internet.[7] As for combatting cybercrime, the United States and its NATO partners are promoting the Budapest Convention, adopted back in 2001.[8]

Such projects undermine inclusive negotiations on these topics held under the auspices of the United Nations.[9] At the global level, there is a competition of approaches to the development of norms and rules underlying the regulation of ICT security. International cooperation in this sphere takes the form of a complex of regimes that includes many global, regional, functional, and transnational governmental systems that often intersect, and in some cases, contradict each other. In the absence of uniform, internationally agreed upon rules of the game, we are witnessing attempts by a number of states to shift responsibility for cyber incidents to their rivals,[10] as well as an intensification of the political and military use of ICT, which only hurts international security. The existence of competing regimes opens up the possibility of manipulating the choice of institutions, and also implies that states are able to pick and choose how they fulfil the obligations they have assumed.

The difficulties that the United Nations is currently facing have meant that transregional governance institutions, including the G20 and BRICS, are becoming increasingly relevant (Lebedeva, Kuznetsov 2019). The possibility of developing solutions to such complex issues as ensuring ICT security on alternative platforms is a popular topic for research. BRICS has an impressive portfolio of decisions that have been developed, agreed upon, and implemented despite differences between the participants (for example, the BRICS New Development Bank was established through the joint efforts of the parties (Kuznetsov 2020). Originally conceived as a group of fast-growing economies, BRICS today covers a wide range of issues and its agenda continues to expand (Larionova et al 2020). The Russian researcher Viktoria Panova has noted that BRICS is taking bold steps towards intensifying cooperation in international security (Panova 2015: 121). This involves, first of all, coordinating foreign policy positions on issues related to ensuring international security. Although initiatives to create institutions have been so far less successful (Abdenur 2017: 73).

---

[7] Declaration for the Future of the Internet. URL: https://www.state.gov/declaration-for-the-future-of-the-internet (accessed: 18.05.2023).

[8] The Budapest Convention (ETS No. 185) and its Protocols. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed: 18.05.2023).

[9] Speech by the Minister of Foreign Affairs of the Russian Federation at the UN Security Council. 20.04.2023. URL: https://www.mid.ru/ru/press_service/video/view/1865243/?TSPD_101_R0=08765fb817ab200019f48a794223f3ad630c5f6c18894fc02a2a55893b58e8859b2bc1adf9f1fba4089f16b658143000c5ddcd0cd3f040911f2e005d76f69b49bfa9c1626a778f40566660464437cc8a2f04a9708c92f97451d80ad99e4fcc7c (accessed: 17.12.2023).

[10] We are talking about the politicization of the process of attributing cyber incidents, and the possibility of unfounded and unconfirmed accusations occurring. See: U.S. Accuses Russia of Cyberattacks on Ukrainian Banks // Interfax. 18.02.2022. URL: https://www.interfax.ru/world/823034 (accessed: 29.08.2022); Taiwan Accuses China of Targeted Plans to Invade the Island // MK. 9.08.2022 URL: https://www.mk.ru/politics/2022/08/09/tayvan-obvinil-kitay-v-celenapravlennoy-podgotovke-vtorzheniya-na-ostrov.html (accessed: 29.08.2022).

The BRICS countries are quick to highlight the fundamental differences in their positions with Western countries on a number of global governance issues, including in the digital space. In this context, the association can be seen as a kind of laboratory for testing the foreign policy initiatives of a group of countries eager to become a leader in global norm-setting. This article attempts to answer the question of the role that BRICS can play in the establishment of a global information security regime within the United Nations.

In terms of its structure, this paper is divided into three parts. We start by defining the basic concept for the topic under consideration – ICT security. Having reviewed existing approaches to defining the subject area of international information security, we propose an adjusted definition of this concept that more accurately reflects the differences between cybersecurity and information security. It also aligns with the approach taken by the BRICS countries in this area. Then we present the theoretical and methodological foundations of the study. Specifically, we use the theory of international regimes and the methodological apparatus developed by the researchers at the University of Toronto to identify, monitor, and give an expert assessment of how effectively informal institutions are fulfilling their global governance obligations. Next, we examine the priorities of the BRICS countries in ICT security – we determine the main focus of each member in this area, compare them and draw conclusions regarding their compatibility. We then analyse multilateral decisions taken by BRICS on ICT security. By identifying politically binding decisions and analysing the results of the subsequent monitoring and assessment by BRICS of the implementation of collective commitments, and then comparing these decisions with the findings of the second section of this paper, we arrive at a conclusion regarding the real prospects for developing multilateral decisions on ICT security within BRICS and the nature of the BRICS countries' influence on the formation of a global information security regime.

The Concepts of "International Information Security," "Cybersecurity," and "ICT Security"

To study the role of BRICS in the formation and evolution of the ICT security regime, we first need to define the terms we will be using – that is, we need to outline the approach to the regulation of the international regime we are looking at. At the same time, the terminology used in this area is itself the subject of heated international debate (Zinovieva, Mishhishina 2022).

The Fundamentals of State Policy of the Russian Federation on International Information Security adopted in 2021 offers the following definition: "International information security is a state of the global information space in which, on the basis of generally recognized norms and principles of international law and on terms of equal partnership, the maintenance of international peace, security, and stability is

ensured."[11] Russia has adopted a broad interpretation of threats to international information security, which encompasses protecting networks, systems, and data (information and technical security), as well as a wider range of issues related to controlling the content of information networks (political and ideological security). The majority of Russian experts take a similar approach to defining threats and what exactly constitutes "international information security" (Boyko 2019; Krutskikh 2022; Romashkina 2022).

At the same time, difficulties arise when it comes to distinguishing between the concepts of information security and cybersecurity:[12] in some studies they are completely mixed up and used arbitrarily, with no indication of the methodical differences between the two (Kartskhiya 2014; Malyuk, Polayanskaya 2016; Khabrieva, Rujpin 2017; Romashkina 2020).[13] A consensus is only just starting to appear among Russian experts regarding the relationship between the subject areas of the two concepts, specifically that cybersecurity is a semantic subspace of information security (Kadulin, Klochkova 2017: 7–8). Most researchers interpret information security as a broader concept than cybersecurity, which aligns fully with the official position.

Outside of Russia, experts do differentiate between these two concepts. However, the subject of cybersecurity in these works appears to extend further than that of information security. For example, (von Solms, Niekerk 2013) identity a common generic root of the concepts – the security of something, going on to clarify that cybersecurity covers a wider range of threats, vulnerabilities, and assets that are subject to security actions. Information in this understanding is a key protected asset, which implies a similar list of threats and vulnerabilities that affect the confidentiality, integrity, and availability of information to varying degrees. At the same time, cybersecurity can address issues of protecting individuals from targeted harmful influence (cyberbullying), the physical assets of individuals that can be damaged as a result of a breach of information security (such as the failure of smart home appliances), and critical infrastructure from the actions of terrorists or a hypothetical aggressor (von Solms, Niekerk 2013: 3–4). Meanwhile, issues of social and state security in the digital age, which form an important layer of Russian academic literature in this area, remain outside the scope of attention of Western researchers.

International negotiations on the creation of a mechanism for regulating relations in the ICT environment have been held within the framework of six UN Groups of Governmental Experts on International Information Security (UNGGE) and two convocations of the Open-Ended Working Group on International Information Security

[11] Decree No. 213 of the President of the Russian Federation "The Fundamentals of State Policy of the Russian Federation on International Information Security" of April 12, 2021. URL: http://www.scrf.gov.ru/security/information/document114/ (accessed: 17.12.2023).

[12] This is noted in particular by (Massel et al. 2016) when considering issues of Russia's energy security.

[13] It is also worth mentioning here the intersection of the concepts of "information weapons" / "cyber weapons"; "information impact" / "cyber impact," and so on.

(OEWG). These are the most authoritative platforms for coordinating multilateral decisions in this area, although they have not yet fully justified the obligations imposed on them under the mandate – not a single legally binding document on issues of ensuring information security has been signed, although a list of rules for the responsible behaviour of states has been formed as a soft-law step. The OEWG and the UNGGE use the compromise term "security within the scope of use of ICTs and ICTs themselves," or the shorter version "ICT security," which is the term we use in this paper. The terminology is generally similar to the official position of Russia and is based on a broad interpretation of security threats, which include political and ideological, as well as informational and technical, aspects. At the same time, in terms of the subject areas of security, it includes issues of countering military-political threats (developing rules for the responsible behaviour of states in the ICT environment), criminal threats, terrorism, and extremism in the digital space. Because the academic literature in Russia, following the official position, places significant emphasis on the problems of ensuring sovereignty in the ICT environment and the management of the digital space in general, the problematic field of ICT security often includes issues of internet governance at the international level (Zinovieva 2021; Krutskikh 2022). In this paper, we use this term as a compromise between the various approaches.

Despite the importance of these issues, the number of works on developing solutions in the field of ICT security in BRICS is relatively small. And those that do exist often do not differentiate between the concepts of cybersecurity and information security, which means that the BRICS agenda on ICT security is overly broad. For example, in addition to countering virus threats and espionage using ICT (Khabrieva, Rujpin 2017: 132), cybersecurity also includes issues of cultural interaction between the BRICS member countries and information support for state policy in the international dimension (Mikhalevich 2017). It would be more appropriate, therefore, to include in the sphere of ICT only those issues that are directly related to ensuring security from threats in this area, while at the same time keeping this area broad enough to cover issues of technical security, content control, and digital sovereignty, as well as the issue of global internet governance and countering the criminal use of ICT.

Thus, we have identified a number of challenges associated with decision-making on ICT security issues at several levels at once – from defining the subject area to interaction at the level of multilateral global governance institutions. The answer to the key question posed in this paper – What role does BRICS play in establishing the international ICT security regime, and what are the prospects for the further work of the association in this area? – is directly related to the definition of the subject area of ICT security.

Global ICT Security as a Complex of Regimes

This paper is based on the theory of international regimes. The key concept is the international regime as such. The most commonly cited definition of this was formulated by Stephen Krasner: "An international regime is a set of principles, norms, rules,

and decision-making procedures around which actors' expectations converge in a specific area of international relations" (Krasner 1982: 1).

Several important points should be noted here. First, the participants in regimes, primarily states, can negotiate in conditions of international anarchy, and their interaction does not necessarily have to be a "zero-sum game." Second, an established and functioning regime is not a static phenomenon. Both the interests of the parties and the composition of the participants and their understanding of the issue at hand can be subject to dynamic change. Third, while the role of the state in the formation and maintenance of the international regime is certainly prioritized, non-state players are taken into consideration too. Robert Keohane noted that there is a constant field of opportunities in global politics for the formation of an international regime that can establish responsibility for certain legal actions, promote the dissemination of more reliable and complete information, or reduce the associated costs of international interaction.

In this context, the formation of a universal international regime can be considered an important condition for the stable development of ICT. Russia officially supports the creation of an international information security regime within the United Nations, one that would include issues of ensuring the responsible behaviour of states in the global ICT environment, as well as issues of internet governance and counteracting the criminal use of ICT.[14]

Given the growth in the number of international organizations and institutions, researchers are publishing works about the formation of both independent regimes and regime complexes. Describing the current trends in cyberspace regulation, Joseph Nye defined the concept as a set of several international regimes.[15] An important implication of Nye's work is the inclusion of the G7/G8 and G20 groups in the list of players. Consequently, BRICS, as a similar institution, can also be considered a full-fledged participant in the process of forming international regimes.[16] The concept of "regime complex" has become rather widespread in the academic literature (Drezner 2013). The regime complex assumes the existence of several different regimes that intersect, complement each other, and in some cases compete with each other. This situation reduces the effectiveness of global governance due to the competition between different institutions, the potential for individual players to manipulate the choice of institution, and the difficulties of monitoring the fulfilment of obligations taken on under individual regimes (Drezner 2013).

---

[14] Decree No. 213 of the President of the Russian Federation "The Fundamentals of State Policy of the Russian Federation on International Information Security" of April 12, 2021. URL: http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZP-Tuc5TrdHURpA4vpN5UTwM.pdf (accessed: 11.09.2022).

[15] Nye J. S. The Regime Complex for Managing Global Cyber Activities. 2014. URl: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (accessed: 11.09.2022).

[16] Nye wrote the article in 2014, a year before BRICS started active work in this area, which is why the association is not mentioned in his analysis.

This is precisely the trend we are seeing in ICT security, where the competition between regulatory approaches and institutions has emerged. The ICT security regime complex is made up of several subject areas, including the development of responsible behaviour norms for states in the ICT environment, counteracting the criminal use of ICT, the internationalization of internet governance, and the protection of human rights in the digital environment. At the same time, international cooperation in this area represents a set of related and intersecting regimes that are constantly developing.[17]

The fragmentation of the internet has only intensified the competition between the different approaches to internet governance[18]. And this has led to the emergence of competing regimes within a single regime complex. The regimes themselves differ in terms of the configuration of participants (for example, the Paris Call focuses on the participation of businesses and non-state actors, while BRICS and the Shanghai Security Organisation are more concerned with inter-state cooperation), subject areas (for example, the Christchurch Call was devoted exclusively to a discussion of issues of countering digital terrorism and extremism; the International Telecommunication Union focuses on the technical aspects of security; and the United Nations, Shanghai Security Organisation, and BRICS deal with a wide range of issues in ICT security).

At the same time, the most serious contradictions concern the norms and principles underlying ICT security regimes. The United States promotes the principle of the freedom of information transfer, including across state borders. Russia, China, and their partners share of vision of an ICT security regime based on the principle of respect for state sovereignty – that is, they transfer the principles of the Westphalian world order to the digital sphere. The United States seeks to form a unilateral imperial order in the digital environment, eroding the principle of sovereignty. The formation of multipolarity is accompanied by growing international conflict, so competition among various platforms of global governance in the ICT environment, including BRICS, is intensifying.

To sum up, a regime complex in the field of ICT security had taken shape by the mid-2020s. The current situation opens up the possibility of manipulating the choice of institution under the regime complex, which could undermine international stability in the ICT environment. Russia calls for the establishment of a universal ICT security regime under the auspices of the United Nations, with regional and macroregional platforms, including BRICS, playing a significant role in achieving this goal.

[17] Zinovieva E. S. 2019. Mezhdunarodnoe sotrudnichestvo po obespecheniu informacionnoi bezopasnosti: subjekty i tendentsii evolyutsii. [International Cooperation on Information Security Provision: Subjects and Evolution Tendencies]. Doctoral thesis. MGIMO. 362 p. (In Russian).

[18] Fick N., Miscik J. Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet. 2022. URL: https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace (accessed: 16.05.2023).

Methodology for Analysing BRICS ICT Security Priorities

Our analysis of the specifics of the BRICS ICT security agenda is carried out with the help of a research tool developed by experts from the University of Toronto that is used to identify, monitor, and provide an expert assessment of the effective implementation of commitments by informal governance institutions – specifically, the G7/G8, the G20, and BRICS. This approach has gained wide recognition and has been used for many years now (Lesazh 2014; Wang 2022; Kirton, Wang 2022).

The tool allows us to establish and substantiate cause-and-effect relationships between the priorities declared by members of global governance institutions and the agreed communiqués, declarations, and other types of documents produced by them. The task set by the creators of the methodology is to assess the trustworthiness of statements made by leaders following summits and whether it is worth paying attention to the documents (communiqués and declarations) adopted following high-level meetings.

The key concept here is "commitment," which is understood as a separate, specific, politically binding, and publicly expressed statement of intent. Each commitment contains elements of discreteness (an indication of a collective goal and/or instrument for achieving a goal), concreteness (certain abstract results are not accepted as goals – for example strengthening international peace and harmony), political obligation (the expression of collective intention, usually worded "we undertake to…" or something similar), an orientation to the future (work to achieve the goal will be carried out in the period following the adoption of the document enshrining the commitment), and collectiveness (the actors implementing the decision are member countries of the institutions themselves; appeals to international organizations and platforms found in the text are not considered commitments). An example of a commitment is the intention of the BRICS member states to develop multilateral cooperation to expand universal access to digital communications, adopted at the 2015 BRICS Summit in Ufa.[19]

Our study of the ICT security commitments of the BRICS countries and their implementation is based on three groups of sources. The first group consists of strategic documents of the BRICS countries, which we studied in order to identify priorities in terms of individual aspects of ICT security. The second includes documents agreed upon by BRICS leaders during annual summits, starting with the 2015 meeting in Ufa,

[19] "We commit ourselves to focus on expanding universal access to all forms of digital communication and to improve awareness of people in this regard" (Communique of BRICS Ministers of Communications on the outcomes of the meeting on "Expansion of Cooperation in the Field of Communications and ICTs". URL: https://www.ranepa.ru/images/media/brics/ruspresidency2/Communique_BRICS_ICT_ministers.pdf (accessed: 11.09.2022). The monitoring process, the specifics of fact collection and the verification process, as well as the final assessment are described in more detail in a special manual. See: Global Governance Program. Compliance Coding Manual for International Institutional Commitments. 2020. URL: http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf (accessed: 11.09.2022).

up to the New Delhi summit in 2021.[20] And the third group is made up of resolutions and other official UN documents reflecting trends in international cooperation in ICT security at the global level, which made it possible to fit BRICS initiatives into the global context and compare it with current trends in the global ICT security regime.

We chose 2015 as the starting point for our study. Although information security issues had been included in the BRICS agenda and final documents before that (the first mention was in the Action Plan released following the 2013 BRICS Summit in Durban), 2015 was nevertheless selected as the starting point. As the Brazilian researcher Luca Belli notes, the BRICS Ufa Declaration of 2015 can be considered the document that marked the beginning of the BRICS consensus on the need to develop a common policy in digital technologies and cybersecurity (Belli 2021).

Our research thus used the methodology for analysing the implementation of commitments developed by University of Toronto scholars to study BRICS documents published from 2015 onwards. This allowed us to assess the interdependence between the declared priorities of cooperation, the actual decisions taken, the coordination of the policies of the BRICS countries within the United Nations, and the potential for institutionalization of cooperation in this area.

ICT Security Issues in BRICS Decisions

There is no consensus among the BRICS countries regarding the substantive content of the concept of ICT security. Russia, China, and India believe that ICT security involves not only a technical component, but also a content-related component. Brazil[21] and South Africa,[22] on the other hand, focus on the technical aspects of information security, while not excluding the political component of security threats.

The issue of ensuring ICT security was introduced into the BRICS agenda at almost the same time that the broader agenda of promoting the development of the digital economy was separated from issues of scientific and technical cooperation. By 2015, ICT development had started to take shape as an independent policy area in the BRICS member countries. ICT security was consolidated as a separate area of international cooperation during Russia's presidency of the association, when, at the initiative of the host country, the first BRICS Communications Ministers' Meeting was held in

[20] This limited time period for studying the 2015 BRICS agenda is due to the fact that the association's agenda for the development of information and communication technologies, which in a broad sense includes issues of ensuring cybersecurity, was separated from its agenda for scientific and technological development. See: (Larionova et al. 2020).

[21] National Information Security Policy of Brazil 2019. URL: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao (accessed: 15.12.2023).

[22] The National Cybersecurity Policy Framework. 9.12.2015. URL: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed: 14.12.2023).

Moscow. The parties approved a joint communiqué on "Expansion of Cooperation in the Field of Communications and ICTs."[23] The main results of the meeting were included in the final declaration of the Ufa BRICS Summit.[24]

At the 2015 Summit in Ufa, the leaders of the BRICS countries adopted 12 commitments on digital development issues, four of which are directly related to issues of ensuring ICT security. More specifically, the following priority areas of digital cooperation were identified: a) interaction and cooperation in responding to information security emergencies; b) joint research to develop new technologies and ICT-related services; c) promotion of a peaceful, secure, open, trust-based, and cooperative digital and internet space; and d) promotion of the use of innovative telecommunications equipment, the development and implementation of new communications standards and technologies for the purpose of creating an information/digital society and countering cyber threats.[25]

The ICT security initiatives put forward by Russia during its 2015 BRICS presidency were supported by the association's partner countries, most notably China. For example, at the 2017 BRICS Summit in Xiamen, the leaders of the five countries declared their support for the development of internationally recognized and universally acceptable rules governing ICT infrastructure security, data protection, and the internet, and committed to jointly building a reliable and secure network.[26] It was at this Summit that the BRICS Roadmap was adopted, which declares the need for collective agreement on the norms and principles that would form the basis of the global ICT security regime.[27]

Decisions on ICT development were also taken during India's (2016 and 2021), South Africa's (2018), and Brazil's (2019) presidency of BRICS, although they were given less emphasis compared to the years when Russia and China set the agenda for discussions. As per the established rotation procedure, Russia took over presidency of the association again in 2020. Its priorities included continuing the dialogue on ensuring international information security and combatting information crime (along with developing cooperation between BRICS countries in combating terrorism and extremism). A special feature of Russia's 2020 BRICS presidency in terms of the association's agenda on information security issues was that it combined two tracks – that is, it reduced the rather broad ICT security agenda to the narrower task of countering

[23] Communique of BRICS Ministers of Communications on the outcomes of the meeting on "Expansion of Cooperation in the Field of Communications and ICTs". 23.10.2015. URL: https://infobrics.org/files/pdf/24.pdf?ysclid=mg0jns9g1t980956703 (accessed: 15.12.2023).

[24] VII BRICS Summit. Ufa Declaration. 9.07.2015. URL: https://www.mea.gov.in/Uploads/PublicationDocs/25448_Declaration_eng.pdf (accessed December 15, 2023).

[25] Ibid.

[26] BRICS Leaders Xiamen Declaration. 4.09.2017. URL: https://nkibrics.ru/system/asset_docs/data/5a4f/6bcb/6272/695d/471a/0000/original/IX_BRICS_SUMMIT_-_XIAMEN_DECLARATION_SEPTEMBER_4__2017_XIAMEN__CHINA.pdf?1515154379 (accessed: 11.09.2022).

[27] Ibid.

terrorism and extremism. At the same time, it continued to focus on coordinating foreign policy on ICT security at the United Nations, developing a comprehensive agreement on international information security and adopting a convention on combating the criminal use of ICT.

The 2020 BRICS Summit in Moscow led to the adopted of the BRICS Counter-Terrorism Strategy, which included collective decisions on ICT security and the use of ICTs, specifically: a) countering extremist narratives conducive to terrorism and the misuse of the internet and social media for the purposes of terrorist recruitment, radicalization and incitement and providing financial and material support for terrorists; and b) strengthening cooperation against the misuse of information and telecommunication technology for terrorist and other criminal purposes.[28]

Our analysis of BRICS decisions on ICT security issues leads us to several important conclusions. First, Russia and China are the most active member countries when it comes to determining the development of the BRICS agenda as a whole,[29] and in the area of international information security in particular. The presidencies of these countries have seen the largest number of decisions made on these issues, not to mention the most substantive. At the same time, Moscow places greater emphasis on the political component of ICT security issues, while Beijing is more concerned on the economic component and issues of network infrastructure development and data security.

Second, an analysis of the content of the collective decisions taken by the association suggests that the broad agenda of guaranteeing ICT security has been gradually narrowed and shifted to focus on countering extremism and terrorism as an institutionally formalized interaction, which is acceptable for all BRICS members.[30] As regards coordinating foreign policy initiatives, the BRICS countries support the creation of an international information security regime under the auspices of the United Nations.

Third, we cannot ignore the fact that the other BRICS members are far less active in terms of putting forward initiatives on international information security. For example, the presidencies of Brazil (2019), India (2016 and 2021), and South Africa (2018) did not bring about any significant decisions in this area and focused on expressing general support for the agenda proposed by the partners.[31]

---

[28] BRICS Counter-Terrorism Strategy 2020. URL: http://www.brics.utoronto.ca/docs/2020-counterterrorism.html (accessed: 11.09.2022).

[29] For a more detailed analysis of the BRICS internet governance agenda, see: (Ignatov 2022).

[30] See: BRICS Counter-Terrorism Strategy 2020.

[31] For example, the 2021 New Delhi Declaration states that the BRICS countries agree to strengthening "capacities of individual States and international organizations to better respond to new and emerging, traditional and non-traditional challenges, including those emanating from terrorism, money laundering, cyber-realm, infodemics and fake news," and also welcomed the "successful conclusion of the work of the Intergovernmental Expert Group (IEG) on Cybercrime."

The commitments adopted and areas of international cooperation can be classified according to a modified version of the University of Toronto methodology discussed earlier depending on their compliance with the basic criteria presented (Table 1).

To determine how effectively the agreements have been implemented, it would be a good idea to analyse the ICT security priorities and approaches of the BRICS, as well as the decisions taken in this area at the international level.

Table 1

Decisions and Areas of BRICS Cooperation on International Information Security

Area of cooperation	Concreteness	Political obligation	Future-oriented	Collectiveness
Support for the development of norms and rules for the responsible behaviour of states in the ICT space (within the framework of the OEWG)	+	+	+	–
Support for the development of a Convention on Combating the Criminal Misue of ICTs and the UN level	+	+	+	–
Existence of bilateral agreements on international information security	+	+	+	+
Adoption of a BRICS Convention on International Information Security	+	+	+	+
Counteracting terrorism and extremism in the ICT	+	+	+	+

Source: compiled by the authors.

ICT Security Priorities of BRICS Member States

Brazil

Brazil ranks 66th in ICT development according to the International Telecommunication Union's 2017 index.[32] It is one of the most developed states in Latin America and, according to expert estimates, one of the most promising countries in terms of digital technology development.[33] It is for this reason that Brazil is interested in cooperation if information security issues in BRICS. At the same time, Brazil's main priority is capacity building and assistance in developing the ICT sector, including disruptive technologies (Perminov: 1520). What is more, the country is rife with ICT crime,[34] which only makes it more eager to engage in international cooperation in this area.

[32] Measuring the Information Society Report 2017. Volume 1. International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf (accessed: 18.12.2023).

[33] See: Digital trends in the Americas region 2021. International Telecommunications Union. URL: https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-DIG_TRENDS_AMS.01-2021-PDF-E.pdf (accessed: 15.12.2023).

[34] Ibid.

Brazil adopted its Basic National Cybersecurity Strategy in 2020. The strategy combined the key provisions of several documents that defined national priorities in the field of cybersecurity and were relevant at the time, specifically, the National Strategy of Defense (updated in 2012),[35] the 2019 National Information Security Policy,[36] and the 2018 Brazilian Digital Transformation Strategy[37] (Hurel & Lobato 2021). The Brazilian leadership has highlighted among its priority tasks adapting the national legislation to changing conditions, referring specifically to the development of a new classification of cybercrimes and requirements for ensuring cybersecurity for people who work remotely, as well as the drafting of a new bill on cybersecurity. Plans have also been announced for the creation of a centralized cyberthreat management system, the development of national requirements for ensuring cybersecurity at the level of individual users and information input devices for government organizations, the implementation of relevant requirements in supply chain management, public procurement systems, and so on.

Notable results from the 2019 BRICS Summit in Brazil are the host country's initiative to develop bilateral agreements between the BRICS countries on this issue. The final declaration also expresses support for the initiatives of the OEWG and the UNGGE launched in 2019 and emphasizes the importance of the UN's work in combatting the criminal use of ICTs.[38]

In terms of its foreign policy, Brazil prioritizes the development of cooperation in Latin America, along with other areas that are typically mentioned in documents of this level, such as participation in multilateral discussions and concluding relevant international agreements. Brazil's goal to create a centralized cyberthreat management system is unashamedly similar to models adopted in several other countries, in particular the United Kingdom, where a special National Cyber Security Centre has been set up to coordinate the efforts of various government departments, as well as private businesses in this area.[39]

In practice, Brazil's participation in international negotiations on ensuring cybersecurity are directed "outside BRICS" and do not fully align with the Russian position. In 2018, Brazil abstained from voting on the draft resolution "Developments in the field of information and telecommunications in the context of international security"

[35] National Strategy of Defense. The government Brazil, 2008 (updated 2012). Available at: https://www.files.ethz.ch/isn/154868/Brazil_English2008.pdf (accessed December 18, 2023).

[36] Política Nacional de Segurança da Informação. The Government of Brazil, 2019. Available at: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao (accessed September 11, 2022).

[37] Brazilian Digital Transformation Strategy. 2018. Available at: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/digitalstrategy.pdf (accessed December 11, 2023).

[38] XI BRICS Summit Brasilia Declaration. 2019. URL: http://www.brics.utoronto.ca/docs/191114-Braslia_Declaration.pdf (accessed: 18.05.2023).

[39] Hurel L. M.. Cybersecurity in Brazil: An analysis if the national strategy. Ingrapé Institute Strategic Paper 51. 2021. URL: https://igarape.org.br/wp-content/uploads/2021/04/SP-54_Cybersecurity-in-Brazil.pdf (accessed: 15.123.2023).

proposed by Russia to get past the stalemate in the UNGGE negotiations and in which the creation of an OEWG was envisioned, reasoning that there was no point duplicating the work of the UNGGE (Stadnik, Tsvetkova 2021: 75). Brazil wants to remain equidistant from the various participants in the negotiation process, an approach to cyber diplomacy that experts have called "wavering" (Hurel 2022). At the same time, this sharp change of course and the sudden support for the Budapest Convention were partly connected with the rise to power of right-wing politician Jair Bolsonaro.

Representatives from Brazil took part in both the UNGGE negotiations and the two OEWG sessions. While at the federal level Brazil has not officially endorsed the Paris Call for Trust and Security in Cyberspace presented by France in November 2018,[40] the state of Sao Paulo and at least a dozen private companies and civil society organizations in Brazil have expressed support for the initiative. Brazil has similarly not joined the initiatives of the Programme of Action for Advancing Responsible State Behaviour in Cyberspace first proposed by France and Egypt in 2020,[41] and received further embellishment in 2022[42] with the aim of replacing the OEWG with an institutional mechanism of the Programme of Action.

Brazil supports work on the UN Treaty on the Criminal Use of ICTs, but it has also joined the Council of Europe's Budapest Convention, which Russia, China, and South Africa view as inconsistent with the principle of respect for state sovereignty. ICT security thus cannot be considered a foreign policy priority of Brazil, a fact that explains its relative lack of interest in developing and deepening cooperation in this area at the institutional level compared to other BRICS members, as well as its somewhat changeable foreign policy line. Brazil is most interested in combatting ICT crime at the international level.

Russia

Russia has a highly developed digital economy, ranking 45th in the International Telecommunication Union's 2017 ICT Development index and exhibiting a high level of network penetration.[43] As of 2023, Russia had managed to retain its high digital potential, despite the sanctions pressure from the West. In its foreign policy, Russia places an emphasis on ensuring international information security and strengthening digital sovereignty.[44] Russia faces a significant number of attacks in cyberspace, which

[40] Paris Call for Trust and Security in Cyberspace. URL: https://pariscall.international/en/call (accessed: 11.09.2022).

[41] Programme of Action (PoA) for Advancing Responsible State Behaviour in Cyberspace. 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf (accessed: 15.12.2023).

[42] Programme of Action to Advance Responsible State Behaviour in the use of Information and Communications Technologies in the Context of International Security. 2022. URL: https://digitallibrary.un.org/record/3991743?ln=ru (accessed: 15.12.2023).

[43] Measuring the Information Society Report 2017. Volume 1. International Telecommunication Union. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf (accessed: 15.12.2023).

[44] Decree No. 229 of the President of the Russian Federation "On Approval of the Concept of Foreign Policy of the Russian Federation". URL: http://static.kremlin.ru/media/events/files/ru/udpjZePcMAycLXOGGAgmVHQDIoFCN2Ae.pdf (accessed: 18.05.2023).

is why it addresses this issue.[45] Russia is a leader in promoting the subject of information security within the United Nations and BRICS (Krutskikh 2022).

The Russian position on ICT security issues is presented in a wide range of strategic documents, including the National Security Strategy of the Russian Federation,[46] the Doctrine of Information Security of the Russian Federation,[47] the Concept of Foreign Policy of the Russian Federation,[48] the Fundamentals of State Policy of the Russian Federation on International Information Security,[49] and the Strategy of the Information Society Development in the Russian Federation for 2017–2030.[50]

In the international arena, Russia's key task is to form an international information security system in order to effectively counter attempts to use ICT for military and other purposes that are contrary to international law, primarily through the creation of appropriate international legal mechanisms. The National Security Strategy of the Russian Federation places priority on the establishment of an international legal regime for ensuring security in the sphere of ICT use. The Concept of Foreign Policy of the Russian Federation indicates that the capabilities of information and communication technologies are increasingly used to solve foreign policy problems, including in the military-political dimension.[51] Finally, the Strategy of the Information Society Development in the Russian Federation for 2017–2030 contains several important points concerning Russia's activities in the field of ICT security in the international arena. The latter document focuses on the creation of international mechanisms to ensure trust on the internet.[52] ICT security is thus the most important area of Russia's foreign policy, and its long-term goal is to form an international legal regime in this area.

Russia is the most consistent and active supporter among the BRICS members of the development of a universal regulatory framework in the field of ICT security. Moscow initiated the discussion of this issue at the United Nations in 1998,[53] and pro-

---

[45] Interview With Deputy Secretary of the Security Council of the Russian Federation O. Khramov // Security Council of the Russian Federation. 08.04.2022. URL: http://www.scrf.gov.ru/news/allnews/3217/ (accessed: 19.12.2023).

[46] Decree No. 400 of the President of the Russian Federation "On the National Security Strategy of the Russian Federation" of July 2, 2021. URL: http://www.kremlin.ru/acts/bank/47046 (accessed: 11.09.2022).

[47] Decree No. 646 of the President of the Russian Federation "On Approving the Doctrine of Information Security of the Russian Federation" of December 5, 2016. URL: http://kremlin.ru/acts/bank/41460 (accessed: 11.09.2022).

[48] Decree No. 229 of the President of the Russian Federation "On Approval of the Concept of Foreign Policy of the Russian Federation". URL: http://static.kremlin.ru/media/events/files/ru/udpjZePcMAycLXOGGAgmVHQDIoFCN2Ae.pdf (accessed: 18.05.2023).

[49] Decree No. 213 of the President of the Russian Federation "The Fundamentals of State Policy of the Russian Federation on International Information Security" of April 12, 2021. URL: http://www.scrf.gov.ru/security/information/document114/ (accessed: 11.09.2022).

[50] Decree No. 203 of the President of the Russian Federation "On the Strategy of the Information Society Development in the Russian Federation for 2017–2030" of May 9, 2017. URL: https://base.garant.ru/71670570/ (accessed: 11.09.2022).

[51] Decree No. 229 of the President of the Russian Federation "On Approval of the Concept of Foreign Policy of the Russian Federation". URL: http://static.kremlin.ru/media/events/files/ru/udpjZePcMAycLXOGGAgmVHQDIoFCN2Ae.pdf (accessed: 18.05.2023).

[52] Decree No. 203 of the President of the Russian Federation "On the Strategy of the Information Society Development in the Russian Federation for 2017–2030" of May 9, 2017. URL: https://base.garant.ru/71670570/ (accessed: 11.09.2022).

[53] United Nations General Assembly Resolution A/RES/53/70 "Developments in the field of information and telecommunications in the context of international security" of December 4, 1998. URL: https://digitallibrary.un.org/record/265311?ln=ru (accessed: 15.12.2023).

posed the initiative to convene the OEWG when negotiations in the UNGGE format stalled. The content of the resolution on cybersecurity issues was developed thanks to Russia's efforts not only in the United Nations, but also in the Shanghai Cooperation Organisation, which contributed to the achievement of an international consensus on the establishment of an additional negotiating format.[54]

The Concept of the Participation of the Russian Federation in BRICS, approved by the President of the Russian Federation in February 2013,[55] sets out Russia's main goals in its cooperation with the BRICS member states on issues of international security. Among these are: cooperating towards ensuring international information security; harnessing the capabilities of BRICS to promote initiatives in this area at various international platforms and organizations, primarily the United Nations; and strengthening cooperation within BRICS to counter the use of ICT for military, terrorist, and criminal purposes, as well as for purposes that run counter to the provision of international peace, stability, and security. Russia thus attaches great significance to developing and deepening cooperation within BRICS on issues of international information security.

In late 2021, Russia and the United States presented a joint draft resolution on cybersecurity issues, which was approved by the General Assembly without a vote.[56] The resolution established the possibility of developing additional mandatory rules of conduct for states in cyberspace, with a proviso "if necessary." Guided by considerations of the need to create broad formats for regulating relations in cyberspace against narrow "coalitions of the willing," which could be formed as a result of the French initiative mentioned above, Russia was not among those who supported the Paris Call (Chikhachev 2022), although several major Russian IT companies declared their support for it.

At the 77th session of the UN General Assembly in 2022, Russia submitted a draft resolution on "Developments in the field of information and telecommunications in the context of international security"[57] for discussion. The resolution was aimed at continuing the work of the UN OEWG beyond 2023. China was the only BRICS member country to co-sponsor the document.[58]

Russia champions international cooperation on issues of international information security at the BRICS level, and the range of issues it includes in this area is extensive, including countering military and political threats, ICT crime and extremism

[54] Russia and SCO Countries to Present Draft UNGA Resolution on Cybersecurity // TASS. 14.12.2017. URL: https://tass.ru/politika/4811804 (accessed: 11.09.2022).

[55] Concept of the Participation of the Russian Federation in BRICS. Approved by the President of the Russian Federation in 2013. URL: http://static.kremlin.ru/media/events/files/41d452a8a232b2f6f8a5.pdf (accessed: 15.12.2023).

[56] UN General Assembly Adopts Russia–U.S. Cyberspace Resolution // TASS. 07.12.2021. URL: https://tass.ru/mezhdunarodnaya-panorama/13127057 (accessed: 11.09.2022).

[57] UN General Assembly Adopts Several Russian Resolutions on Security and Disarmament // TASS. 08.12.2022. URL: https://tass.ru/mezhdunarodnaya-panorama/16533015 (accessed: 18.05.2023).

[58] Chernenko E. Manhattan Projects: How Russia and Western Countries are Pushing Competing Cybersecurity Resolutions at the UN // Kommersnat. 07.11.2022. URL: https://www.kommersant.ru/doc/5651792 (accessed: 18.05.2023).

on the internet, protecting digital sovereignty from external interference, and issues of internet governance. In the long term, Russia is guiding the international community and BRICS towards concluding legally binding agreements on ICT security at the global and regional levels.

India

India is one of the world's largest providers of information and communications services. But this does not mean that the country has a highly developed system of priorities and action plans in the ICT field. This can be explained by the fact that, until recently, the Indian leadership did not attach any real importance to the risks of confrontation in the digital space.[59] In fact, the full-fledged development of a system to counter emerging threats only began in 2018, meaning that there are only two doctrinal documents available for analysis – the National Security Strategy and the National Digital Communications Policy.

India's National Security Strategy contains a short list of threats and suggests areas of action in ICT security.[60] Among the threats named in the Strategy are cybercrime, the possibility of using cyber weapons elements of the country's critical infrastructure, and the use of social media to influence the population "to sow discord amongst people, spread propaganda and weaken faith in the government."[61] Unprotected personal data is seen as a risk of the dissemination of personal false information. Key tasks in this regard include implementing requirements for the localization of user data; drawing up a more detailed list of steps to counter the use of cyber weapons, in particular the creation of a single decision-making centre (a cyber command); and building up cyber-attack detection capabilities, with cyber-attacks themselves being classified as unfriendly acts and a violation of state sovereignty.

The National Digital Communications Policy highlights the economic potential of ICT and, as such, emphasizes the priority of protecting the "digital sovereignty" of the state.[62] This includes, first of all, taking steps to protect user date from unauthorized access, supporting local service and product providers, increasing the effectiveness of communications product licensing bodies, and promoting national interests in the context of formulating international industry standards. In terms of data security issues, India's policy appears to be similar to China's position, and the emphasis on digital sovereignty brings its stance closer to that of Russia.

---

[59] Kupriyanov A. V. India in the Era of Cyber Wars // Russian International Affairs Council. 7.08.2019. URL: https://russiancouncil.ru/analytics-and-comments/analytics/indiya-v-epokhu-kibervoyn/ (accessed: 4.08.2022).

[60] India's National Security Strategy. 2019. URL: https://manifesto.inc.in/pdf/national_security_strategy_gen_hooda.pdf (accessed: 11.09.2022).

[61] Ibid.

[62] National Digital Communications Policy. 2018. URL: https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf (accessed: 11.09.2022).

India supports the inclusion of ICT security issues in the UN and BRICS agendas. It is no coincidence that the theme of the 2021 BRICS Summit in India was "BRICS Partnership for Global Stability, Security, and Prosperity." At the same time, India placed an emphasis on cooperation in the fight against terrorism. The document also notes the importance of cooperation in ICT security and asserts the need to work towards "a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries."[63] Special emphasis is placed on the central role of the United Nations in this area and support for work on developing a comprehensive convention on countering the use of ICTs for criminal purposes.[64] At the same time, India also supports the cooperation formats proposed by Western countries, including the most recent convocation of the UNGGE. India has not formally joined the Paris Call,[65] although more than 50 private companies and civil society organizations in the country have expressed their support for the non-binding set of principles contained in it. This is more than any other BRICS country. India, along with China, did not support the resolution proffered by Russia and the United States in 2021. Nor did it support the Programme of Action for Advancing Responsible State Behaviour in Cyberspace proposed by France in 2020,[66] or the Declaration for the future of the Internet put forward by the United States in 2022.[67] However, India did vote in favour of UN General Assembly Resolution 77 proposed by France on a "Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security,"[68] as an alternative to the Russia-led OEWG initiative.[69]

India views ICT as a critical driver of economic growth and development and is thus interested in cooperation on ICT security, including the formation of an international legal regime under the auspices of the United Nations based on the principles of respect for digital sovereignty, as well as the conclusion of a formal agreement on ICT security in BRICS. Another important priority for India is combatting the criminal use of ICTs and digital terrorism. Despite the fact that India is forced to take the position of Western countries that promote an alternative vision of the cybersecurity regime

[63] XIII BRICS Summit. New Delhi Declaration. 2021. URL: https://www.ranepa.ru/ciir/briks/predsedatelstva/briks-indiyskoe-predsedatelstvo-2021g/New%20Delhi%20Declaration%202021%20RUS.pdf (accessed: 11.09.2022).
[64] Ibid.
[65] Paris Call for Trust and Security in Cyberspace. 2018. URL: https://pariscall.international/en/ (accessed: 15.12.2023).
[66] Programme of Action for Advancing Responsible State Behaviour in Cyberspace. 2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf (accessed: 15.12.2023).
[67] Declaration for the Future of the Internet. 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf (accessed: 15.12.2023).
[68] Programme of Action to Advance Responsible State Behaviour in the Use of Information and Communications Technologies in the Context of International Security. 2022. URL: https://digitallibrary.un.org/record/3991743?ln=ru (accessed: 15.12.2023).
[69] Zinovieva E. S. International Information Security in US-Russian Bilateral Relations. Russian International Affairs Council. 2022. URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-v-dvustoronnikh-otnosheniyakh-rossii-i-ssha/?sphrase_id=98721820 (accessed: 18.05.2023).

into account, in many respects its priorities in the field of ICT align fairly well with the stances taken by Russia and China, which increases its interest in institutionalizing interaction and supports active cooperation within BRICS on issues of ICT security.

China

China is a recognized leader in cyberspace regulation, and the country's approach to this issue can be described as among the most stringent in relation to ensuring digital sovereignty. China (along with the United States) leads the way when it comes to developing disruptive technologies,[70] including Big Data, the Internet of Things, and machine learning. China is implementing its Belt and Road Initiative, which includes a Digital Silk Road component that is aimed at building digital infrastructure in developing countries.[71] The economic aspects of digital development are thus a priority for China, but implementing them requires ensuring a high level of security.

The regulatory framework for China's policy in this area started to take shape with the establishment of the National Coordination Group on Cybersecurity and Information Security, which led to the first iteration of a specialized national strategy (Romashkina & Zadremaylova 2020: 124). The current version of the Strategy, adopted in 2016,[72] sees cyberthreats as one of the main obstacles to economic growth and political and economic security. Among the possible consequences of the use of ICT capabilities for illegal and hostile actions, the document mentions the disruption of critical infrastructure (the transport and energy infrastructure in particular), the dissemination of false information, civil unrest, and the overthrow of existing regimes. As a countermeasure, the Chinese government controls online activity in order to suppress illegal activities (especially calls for civil disobedience and separatism), strengthen socialist values as an integral element of online culture, and develop a talent pool and national technological base. The Counterterrorism Law of the People's Republic of China (2015),[73] the China Cybersecurity Law (2016),[74] and the Regulations on the Security Protection of Critical Information Infrastructure (2021)[75] provide the legal basis for these activities.

[70] UNCTAD Digital Economy Report // UNCTAD. 2021. URL: https://unctad.org/publication/digital-economy-report-2021 (accessed: 15.12.2023).

[71] Action Plan on the Belt and Road Initiative // The State Council of the People's Republic of China. 2015. URL: https://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm (accessed: 15.12.2023).

[72] Unofficial translation of the National Cyberspace Security Strategy. URL: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (accessed: 11.09.2022).

[73] Counterterrorism Law of the People's Republic of China (Order No. 36 of the President of the PRC). URL: https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=103954&p_country=CHN&p_count=1189 (accessed: 11.09.2022).

[74] Unofficial of the China Cybersecurity Law. URL: https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (accessed: 11.09.2022).

[75] Gong J., Yue C. 2021. China Released Regulation on Critical Information Infrastructure // Bird & Bird. 06.09.2021. URL: https://www.twobirds.com/en/insights/2021/china/china-released-regulation-on-critical-information-infrastructure (accessed: 11.08.2022).

In June 2021, Beijing passed a new Data Security Law that establishes stricter requirements for the processing of important data, key government data, and sensitive data, extends the requirement to comply with the Cyber Security Law's Multi-Level Protection Framework to all automated data processing, and broadens data localization obligations to include the important data categories already mentioned.[76]

China's foreign policy priorities in ICT security are further elaborated in the International Strategy of Cooperation on Cyberspace, adopted in 2017,[77] which enshrines the principles of non-pursuit of cyber hegemony, non-interference in the internal affairs of other countries using ICT capabilities, and the priority of realizing state sovereignty in the information space (Romashkina, Zadremaylova 2021: 130). The authors of the Strategy call for the creation of a system for regulating relations in cyberspace based on agreed rules and norms developed on the basis of equal participation and non-discrimination.

In 2020, China rolled out its Global Initiative on Data Security,[78] which postulates the importance of sovereignty in the digital space and the central role of the United Nations in data governance and ensuring international information security.

China did not co-sponsor the U.S.–Russian resolution put forward in 2021, nor did it support Western initiatives in this area. For example, like the other BRICS countries, China has not officially supported the Paris Call at the state level. And among representatives of the private sector and civil society, only one company has openly expressed support for the initiative. As for the highly politically motivated initiatives of the United States and Western countries – for example, the Declaration for the Future of the Internet[79] and the Programme of Action for Advancing Responsible State Behaviour in Cyberspace[80] – China has expressed its unequivocal opposition to them.

Issues of ensuring information security were at the forefront of discussions at the 2022 BRICS Summit in Beijing. Specifically, the Beijing Declaration emphasized "the need to advance practical intra-BRICS cooperation through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring security in the use of ICTs and the activities of the BRICS Working Group on security in the use of ICTs."[81] The document also notes the progress made in the work of the UN Open-Ended Ad Hoc Committee of Experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes.[82]

---

[76] Data Security Law of China. 2021. URL: https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (accessed: 15.12.2023).

[77] International Strategy of Cooperation on Cyberspace. 2017. URL: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm (accessed: 11.09.2022).

[78] Global Initiative on Data Security. 2020. URL: https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405182.html (accessed: 18.05.2023).

[79] Declaration for the Future of the Internet. 2022. URL: https://www.state.gov/declaration-for-the-future-of-the-internet (accessed: 18.05.2023).

[80] General Assembly official records, 77th session: 46th plenary meeting. 07.12.2022. URL: https://digitallibrary.un.org/record/4009684?ln=en (accessed: 18.05.2023).

[81] XIV BRICS Summit Beijing Declaration. 23.06.2022. URL: http://www.kremlin.ru/supplement/5819 (accessed: 15.12.2023).

[82] Ibid.

Thus, the positions of Russia and China regarding the main parameters of international cooperation in the field of ICT security are extremely close. Both countries advocate the creation of an international regime in this area based on the Westphalian principles of respect for sovereignty, placing it in opposition to the initiatives promoted by the United States and its allies. Other important aspects of China's position are the fight against the use of ICTs for criminal purposes and terrorist acts and the protection of data, which is considered the most important resource for technological and economic development.

South Africa

South Africa is a leader in digital development in the African region (Pantzerev 2018:14). However, the issue of ensuring cybersecurity is only developed at the surface level in the country's official documents and strategies, despite the diversity of the threats that exist in this area. The National Cybersecurity Policy Framework was adopted in 2015. At the time, South Africa was already among the highest-ranked countries in terms of the number of online fraud incidents and other internet-related crimes.[83] The main threats to cybersecurity identified by the authors of the National Cybersecurity Policy Framework led them to the conclusion that equipment and technologies that are important for ensuring an adequate protection need to be imported into the countries. The lack of experts capable of countering the increasing number of cyber incidents in the previous years was also noted. The document proposed establishing effective coordination of the actions of state bodies, as well as a specialized coordinating body. The main coordinating functions were assigned to the Cybersecurity Hub, which was also responsible for developing strategic documents.

The process of adapting South Africa's national legislation to the realities of the spread of cybercrime has taken quite a long time. The first draft of the Cybercrime Law was presented in August 2015. The revision process took about a year and a half, meaning that it was only sent to parliament for consideration in early 2017. The original version of the law was strongly supported by President Jacob Zuma's followers, but it was met with strong opposition. Many believed that that it did not differentiate "between espionage and an act of journalism" and, given the increasing number of scandals involving members of the Zuma administration, could be used to exert pressure on the media.[84] After Zuma's resignation and allegations of corruption,[85] the draft

[83] The National Cybersecurity Policy Framework. 2015. URL: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed: 11.09.2022).

[84] Joseph R. South Africa's Cybercrimes and Cybersecurity Bill is deeply flawed // Index or Censorship. 07.01.2017. URL: https://www.indexoncensorship.org/2016/01/raymond-joseph-south-africa-cybercrimes-and-cybersecurity-bill/ (accessed: 11.09.2022).

[85] Burke J. Zuma in the dock: South Africa's ex-president faces corruption charges // The Guardian. 06.04.2018. Available at: https://www.theguardian.com/world/2018/apr/06/south-africa-jacob-zuma-court-corruption-charges (accessed: 06.11.2022).

law was subject to public consultation on two separate occasions, in 2018 and 2019. In later 2020, the bill was supported by both houses of the South African parliament. President Cyril Ramaphosa signed the Act into law in May 2021, and it came into effect on December 1, 2021. Prior to the adoption of the Cybercrime Act, the South African authorities used the provisions of the Criminal Procedure Code, which, coupled with the absence of a clear definition of cybercrime in the law, has made it difficult to investigate crimes committee in cyberspace.[86]

The South African leadership has consistently taken a sceptical position on international agreements concerning ICT security, despite the stated priority of developing international cooperation within the National Cybersecurity Policy Framework. One of the more glaring examples in this respect is the "Afro-sceptic" position taken by South Africa to the African Union Convention on Cyber Security and Personal Data Protection (Orji 2018),[87] refusing to ratify the document.

Like its BRICS partners, South Africa did not endorse the Paris Call, and fewer than twenty private companies and civil society organizations in the country supported it. And while South Africa did support the 2021 draft resolution put forward by the Russian and the United States, it did not join the Programme of Action for Advancing Responsible State Behaviour in Cyberspace. During the 77th Session of the UN General Assembly in 2022, South Africa spoke in support of the Russian draft resolution on international information security. It is also a signatory of the 2001 Budapest Convention on Cybercrime, although this does not prevent it from participating in negotiations at the UN on the development of a Convention on Combatting the Criminal Misuse of ICTs and supporting this initiative at the BRICS level. The Second Johannesburg Declaration of BRICS noted the commitment to continue work on the development of a convention on combatting ICT crime in the UN, as well as the formation of a BRICS legal framework on issues of ensuring security in the use of ICTs.[88]

It is thus clear that South Africa is less interested in developing cooperation in ICT security than other BRICS members, but supports BRICS initiatives in this area at the United Nations, as well as the signing of an intergovernmental agreement within BRICS.

An analysis of the strategies and other important documents related to the national policies of the BRICS countries on ICT security allows us to draw the following conclusions. First, the degree to which the countries of the association have elaborated these issues differs significantly. Russia and China have the most detailed systems of

[86] Allen K. South Africa lays down the law on cybercrime // Institute for Security Studies. URL: https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime (accessed: 11.09.2022).

[87] African Union Convention on Cyber Security and Personal Data Protection. 2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed: 11.09.2022).

[88] XV BRICS Summit Johannesburg II Declaration. 24.08.2023. URL: http://static.kremlin.ru/media/events/files/ru/ls471x-8ogLBhjRQx05ufVB2uzMFo1kWs.pdf (accessed: 15.12.2023).

priorities and tasks in the field of cybersecurity and have therefore gone further than the others member states in terms of legislative support for the various initiatives and actions we have discussed at the national and international levels. Moscow and Beijing are the most active among the BRICS countries in the international discussion of this issue, and among these two, Russia is usually the one coming up with new initiatives. The trio of Brazil, India, and South Africa noticeably lags behind in this regard, which is more or less in line with the estimated level of digital development of the BRICS countries (Ignatov 2020). Second, each of the partners has different priorities when it comes to cybersecurity. Russia, China, and India tend to directly or indirectly treat issues related to the dissemination of information through digital communication networks as part of international information security, which significantly expands the scope of potential threats. The approach of Brazil and South Africa is more practical and involves working primarily with traditional cybersecurity challenges (in particular, the potential for using ICTs as a means of committing cybercrime). Breaking the group into two subgroups – Brazil and South Africa on the one hand and Russia, China, and India on the other – more or less corresponds to the concept of weak digital sovereignty (limited government intervention in ensuring cybersecurity) and strong digital sovereignty (cybersecurity issues are raised to the level of a national security problem and are supported by appropriate actions) discussed in (Ignatov 2022). Despite the fact that these countries are classified in the academic literature as "sovereignty hawks" (Panova 2015), in reality the interpretation by states of the content of digital sovereignty varies somewhat. The emphasis on the importance of digital sovereignty means that little attention is paid to coordinating the activities of non-state BRICS players within the ICT security regime, as the priority is coordination among the states involved.

* * *

This paper successfully tackled a number of research problems. We proposed a more precise definition of the concept of ICT security, which we then used in our discussion of the national priorities of BRICS member countries and the decisions taken within the association in this issue.

Our analysis of the strategic planning documents of the five BRICS member states revealed that they are all committed to the norms of respect for state sovereignty in the ICT environment and see it as the basis of the international regime in this area. This allowed us to divide the BRICS countries into two groups. The first group is made up of Russia, China, and India, which have adopted an approach to ensuring ICT security that includes issues of regulating the content of the global internet and its technical security (this approach is reflected in the terminology used – "international information security" (Zinovieva, Mishhishina 2022), and also pay significant attention to issues of information security. The second group includes Brazil and South Africa, whose position focuses on capacity building and bridging the digital divide. They are less interested in regulating digital content. All five BRICS member states support the

need for international cooperation in combatting the criminal use of ICTs within the framework of the special committee of the UN General Assembly based on respect for the principle of state sovereignty. At the same time, India is more active than Brazil and South Africa when it comes to developing cooperation among the BRICS countries in ICT security. All the BRICS countries are paying increasing attention to issues of data security.

Russia and China effectively determine the direction of multilateral discussions within BRICS on the issue of ICT security. At the global level, Russia is the most active in promoting issues of international information security at the United Nations, while China is more focused on issues of digital technology development and support for its Digital Belt and Road project. India leans more towards Russia in this regard, as it too is inclined to include matters relating to the circulation of information in the digital environment and, importantly, control over its content as part of cybersecurity as a whole. Brazil and South Africa do not consider these tasks to be priorities and are more concerned with how to overcome the digital divide and how to increase their digital technological capacity. What is more, Russia and China are significantly ahead of their partners in terms of setting strategic guidelines and adapting national legislation to the changing international situation.

BRICS is a major player in the process of forming an international cybersecurity regime in terms of developing the basic norms and principles of cooperation supported by all countries within the United Nations. The commonality of approaches of the BRICS states to the formation of the international information security system was confirmed quite clearly during the adoption of the Russian draft resolutions "Developments in the Field of Information and Telecommunications in the Context of International Security" and "Countering the Use of Information and Communications Technologies for Criminal Purposes" at the 73rd Session of the UN General Assembly. We can thus say that in no area is the effectiveness of interaction within BRICS demonstrated better than in coordinating foreign policy courses and supporting initiatives at the United Nations.

The table below shows how the BRICS countries have voted on, and thus participated in, the formation of an international ICT security regime (Table 2). The information contained in the table indicates a high degree of coordination among the BRICS countries of their foreign policies within the United Nations on issues of forming a global ICT security regime. At the same time, in the context of growing international conflict, it seems unlikely that any international agreements will be adopted at the level of the United Nations any time soon. Given this, it would be a good idea to narrow the BRICS agenda on this issue.

Table 2
Voting on the Main Projects and Participation of BRICS Countries in the Formation of an International Security Regime

	Brazil	Russia	India	China	South Africa
Support for the development of a universal treaty on international ICT security (within the framework of the OEWG initiated by Russia)	+	+	+	+	+
Support for the development of a convention on combatting the criminal misuse of ICTs	+	+	+	+	+
The existence of bilateral agreements with Russia on international information security	+	+	+	+	+
Support for Russia's 2022 UNGA Resolution (on extending the OEWG mandate beyond 2025)	+	+	+	+	+
Support for France's 2022 resolution (PoA)	+	–	+	–	+
Support for the Paris Call and the Declaration on the Future of the Internet	–	–	–	–	–
Participation in the 2001 Budapest Convention	–	–	–	–	–

Source: compiled by the authors.

Narrowing the BRICS ICT security agenda to mutually acceptable topics for discussion, such as countering online extremist and terrorism in all its manifestations, will help deepen institutional cooperation within the association. Combatting ICT crime is another priority common to all the BRICS countries, but cooperation in this area is already well established at the UN platform, so it does not really make sense to deepen interaction on this issue within BRICS too, since it could divert resources and attention from the UN process. Advancing Russia and China's positions on ICT security issues that require discussion and multilateral decision-making within BRICS will allow many practical issues to be resolved in the future. One example of this could be the establishment of a broader exchange of information on countering the spread of extremist materials.

Given who is next in the next few rotations of the BRICS presidency, in particular Russia's 2024 chairmanship, it would be wise to steer negotiations towards a more detailed study of issues related to ensuring international information security. Priority could be given to issues concerning the principles of cooperation and confidence-building measures in identifying sources of ICT threats and the functioning of mechanisms for ensuring trust and verifying actions in the ICT space. Another important point is to agree on a position regarding the initiative of UN Secretary General António Guterres – that is, the adoption by the United Nations of the Global Digital Compact,

which is expected to cover much of the same ground as the Russia-led UN OEWG. This approach could help further promote the BRICS consensus position within larger platforms, the United Nations in particular.

It is difficult at the present juncture to speak with any certainty about the prospects for a rapprochement of positions with the new BRICS member states on issues of ICT security. Some of them, for example Argentina and Saudi Arabia, have experience participating in multilateral G20 initiatives alongside BRICS member states, while Egypt, Iran, Ethiopia, and the United Arab Emirates do not. At the same time, we can assume that Iran, which has been actively increasing its own cyber potential in recent years[89], will likely back the approach of Russia and China in order to maximize its digital sovereignty. The prospects for further rapprochement of the expanded BRICS on issues of ensuring ICT security will largely depend on how effectively Russia is able to get the members to coordinate their positions during its upcoming presidency of BRICS in 2024.

About the Authors:

Elena S. Zinovieva – Doctor of Political Sciences, Professor, MGIMO University, 76, Prospect Vernadskogo Moscow, Russia 119454. E-mail: zinovjeva@mail.ru

Alexander A. Ignatov – Postgraduate Student, MGIMO University, 76, Prospect Vernadskogo Moscow, Russia 119454; Research Fellow, Center for Research of International Institutions, Russian Presidential Academy of National Economy and Public Administration, 84, Prospect Vernadskogo Moscow, Russia 103274.

Conflict of interest:
The authors declare the absence of conflicts of interest.

References:

Abdenur A. 2017. Can BRICS Cooperate in International Security? *Vestnik mezhdunarodnykh organizatsij.* No. 12(3). P. 73–95.

Alpeev A. S. 2014. Terminologiia bezopasnosti: kiberbezopasnost', informatsionnaia bezopasnost' [Terminology of Security: Cybersecurity, Information Security]. *Voprosy kiberbezopasnosti.* No.5(8). P. 39–42. (In Russian).

Belli L. (Ed.) 2021. *CyberBRICS: Cybersecurity Regulations in the BRICS Countries.* Cham: Springer Nature. 280 p.

Bezkorovajnyj M. M., Tatuzov A. L. 2014. Kiberbezopasnost' - podkhody k opredeleniiu poniatiia [Cybersecurity: Approaches to the Definition]. *Voprosy kiberbezopasnosti.* No. 1(2). P. 22–27. (In Russian).

Boiko S. M. 2019. Problematika mezhdunarodnoi informatsionnoi bezopasnosti na ploshchadkakh ShOS i BRIKS [Problems of International Information Security at the SCO and BRICS Platforms]. *Mezhdunarodnaya zhizn'.* No. 1. P. 1–22. (In Russian).

[89] Khegaturov A. Iran's Cyberpower. Russian International Affairs Council. 19.03.2019 URL: https://russiancouncil.ru/activity/digest/longreads/kibermoshch-irana/ (accessed: 19.12.2023).

Bukht R., Hiks R. 2018. Opredelenie, konceptsiya i izmerenie tsifrovoi ekonomiki [Defining, Conceptualising and Measuring the Digital Economy]. *Vestnik mezhdunarodnyh organizacii.* No. 13(2). P. 143–172. (In Russian). DOI: 10.17323/1996-7845-2018-02-07

Chikhachev A. Y. 2022. Rossiisko-francuzskie otnosheniia pri prezidente Jemmaniuele Makrone: dostizhenia i protivorechia [Russia–France Relations During E. Macrons's Term: Achievements and Challenges]. *Vestnik of Saint Petersburg State University. International Relations.* 15. P. 86–104. (In Russian).

Hurel L. M., Lobato L. C. 2020. Cyber security in Brazil: keeping silos or building bridges? In: S. N. Romaniuk, M. Manjikian (Eds.) *Routledge Companion to Global Cyber-security Strategy.* London: Routledge. 656 p.

Ignatov A. A. 2020. Tsifrovaya ekonomika v BRIKS: Perspektivy mezhdunarodnogo sotrudnichestva [The Digital Economy of BRICS: Prospects for Multilateral Cooperation]. *Vestnik mezhdunarodnyh organizatsii.* No. 15(1). P. 31–62. (In Russian). DOI: 10.17323/1996-7845-2020-01-02

Ignatov A. A. 2022. Upravlenie Internetom v povestke BRIKS [The BRICS Agenda on the Internet Governance]. *Vestnik mezhdunarodnyh organizatsii.* No. 17(2). P. 86–109. (In Russian). DOI: 10.17323/1996-7845-2022-02-04

Kadulin V. E., Klochkova E. N. 2017. Sootnoshenie ponyatii "informacionnaya bezopasnost'" i "kiberbezopasnost'" v sovremennom pravovom pole [Correlation of the Terms "Information Security" and "Cybersecurity" in Modern International Law]. *Voprosy kiberbezopasnosti.* No. 2(20). P. 7–10. (In Russian).

Karchija A. A. 2014. Kiberbezopasnost' i intellektual'naia sobstvennost'. Chast' 1 [Cybersecurity and Intellectual Property. Part 1]. *Voprosy kiberbezopasnosti.* 1(2). P. 61–66. (In Russian).

Karpova D. N. 2014. Kiberprestupnost': global'naia problema i ee reshenie [Cybersecurity: Global Problem and Solution]. *Vlast'*. No. 8. P. 46–50. (In Russian).

Khabrieva T. Y., Rujpin, D. (Eds.) 2017. *Kiberprostranstvo BRIKS: pravovoe izmerenie* [BRICS Cyberdomain: Legislative Framework]. Moscow: Institut zakonodatel'stva i sravnitel'nogo pravovedeniia pri Pravitel'stve Rossiiskoi Federacii. 336 p. (In Russian).

Kirton J., Wang A. X. 2022. China's Complex Leadership in G20 and Global Governance: From Hangzhou 2016 to Kunming 2021. *Chinese Political Science Review.* No. 8. P. 331–380. DOI: https://doi.org/10.1007/s41111-022-00213-9

Krasner S. 1982. Regimes and the limits of realism: Regimes as autonomous variables. *International Organization.* No. 36(2). P. 497–510.

Krutskikh A. V. 2007. K politiko-pravovym osnovaniiam global'noi informacionnoi bezopasnosti [On the Political and Normative Foundations of Global Information Security]. *Mezhdunarodnye process.* No. 5(1;13). P. 28–37. (In Russian).

Krutskikh A. V. 2022. Mezhdunarodnaia informacionnaia bezopasnost': v poiskah konsolidirovannyh podhodov [International Information Security: In Search for Consolidated Approaches]. *Vestnik RUDN. International Relations.* No. 22(2). P. 342–351. (In Russian).

Krutskikh A. V., Streltsov A. A. 2014. Mezhdunarodnoe pravo i problema obespecheniya mezhdunarodnoi informacionnoi bezopasnosti [International Law and the Issue of International Information Security Provision]. *The International Affairs.* No. 11. P. 20–34. (In Russian).

Kuznetsov D. A. 2020. Setevaya tekstura mirovoi politiki: transregionalizm BRIKS [Network Texture of World Politics: Transregionalism of BRICS]. *World Economy and International Relations.* No. 64(11). P. 124–131. (In Russian).

Larionova M. V., Ignatov A. A., Popova I. M., Saharov A. G., Shelepov A. V. 2020. *Desiat' let BRIKS: chto dal'she?* [BRICS at Ten: The Way Forward]. Moscow: Delo. 73 p. (In Russian).

Lebedeva M. M., Kuznetsov D. A. 2019. Transregionalizm – novyi fenomen mirovoi politiki. [Transregional Integration as a New Phenomenon of World Politics: Nature and Prospects]. *Polis. Politicheskie issledovaniya.* No. 5. P. 71–84. (In Russian). DOI: 10.17976/jpps/2019.05.06

Lesazh D. 2014. Tekushhaya programma deistvii «Gruppy dvadcati» v sfere nalogooblozheniya: ispolnenie objazatel'stv, otchetnost' i legitimnost' [The Current G20 Taxation Agenda: Compliance, Accountability and Legitimacy]. *Vestnik mezhdunarodnyh organizatsii.* No. 9(4). P. 40–54. (In Russian).

Malyuk A. A., Polyanskaya O. Y. 2016. Zarubezhnyi opyt formirovaniya v obshhestve kul'tury informacionnoi bezopasnosti [Fostering Information Security Culture: International Experience]. *Bezopasnost' informacionnyh tehnologij.* No. 23(4). P. 25–37. (In Russian).

Massel' L. V., Voropaj N. I., Senderov S. M., Massel' A. G. 2016. Kiberopasnost' kak odna iz strategicheskih ugroz jenergeticheskoi bezopasnosti Rossii [Cybersecurity as One of Strategic Threats to Russia's Energy Security]. *Voprosy kiberbezopasnosti.* No. 4(17). P. 1–10. (In Russian).

Mikhalevich E. A. 2017. Rossiysko-kitajskoe vzaimodeistvie po obespecheniu bezopasnosti v kiberprostranstve v ramkah BRIKS [Russia–China Cooperation in Cybersecurity Provision within BRICS]. *Svobodnaja mysl'*. No. 6(1684). P. 155–160. (In Russian).

Orji U. J. 2018. The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology.* No. 12(2). P. 91–130. DOI: https://doi.org/10.5817/MUJLT2018-2-1

Panova V. V. 2015. Problemy bezopasnosti i perspektivy sammita BRIKS v Ufe [The BRICS Security Agenda and Prospects for the BRICS Ufa Summit]. *Vestnik mezhdunarodnyh organizacii.* No. 10(2). P. 119–139. (In Russian).

Perminov V. A. 2019. Sektor informacionno-kommunikacionnyh tehnologii Brazilii: istoriya, sovremennoe polozhenie i tendencii razvitiua [Information and Communication Technologies Sector in Brazil: History, Current State of Affairs, and Development Prospects]. *Ekonomicheskie otnosheniya.* No. 9(3). P. 1519–1532. (In Russian).

Romashkina N. P. 2020. Problema mezhdunarodnoi informacionnoi bezopasnosti v OON [International Information Security Issue at the UN]. *Mirovaya ekonomika i mezhdunarodnye otnosheniya.* No. 64(12). P. 25–32. (In Russian).

Romashkina N. P., Zadremajlova V. G. 2020. Evoljutsiya politiki KNR v oblasti informacionnoi bezopasnosti [China's Information Security Policy Evolution]. *Put' k miru i bezopasnosti.* No. 1(58). P. 122–138. (In Russian). DOI: 10.20542/2307-1494-2020-1-122-138

Stadnik I. T., Tsvetkova N. A. 2021. Mesto i rol' stran Latinskoi Ameriki v sisteme mezhdunarodnoi i regional'noi kiberbezopasnosti [Latin American Countries Position Within Regional and Global Cybersecurity Systems]. *Latinskaya Amerika.* No. 4. P. 69–84. (In Russian).

Wang A. S. 2022. Model' liderstva Kitaya v BRIKS [China's Leadership in BRICS Governance]. *Vestnik mezhdunarodnykh organizatsii.* No. 17(2). (In Russian). P. 50–85. DOI: 10.17323/1996-7845-2022-02-03

Zgoba A. I., Markelov D. V., Smirnov P. I. 2014. Kiberbezopasnost': ugrozy, vyzovy, resheniya [Cybersecurity: Threats, Challenges, Solutions]. *Voprosy kiberbezopasnosti.* No. 5(8). P. 30–38. (In Russian).