The BRICS Agenda on Internet Governance[1]

A. Ignatov

Alexander A. Ignatov—PhD student, MGIMO University; researcher, Center for International Institutions Research (CIIR), Russian Presidential Academy of National Economy and Public Administration; 119034, Russia, Moscow, 11 Prechistenskaya Naberezhnaya, office 403. +7 4956951179. E-mail: ignatov-aa@ranepa.ru

Abstract

The key features of the modern Internet governance system are its decentralized structure, inhomogeneous internal "geography," and the diverse nature of its decision-making actors. These factors determine the complexity of the decision-making process on Internet governance-related issues. Under these conditions, the BRICS group of Brazil, Russia, India, China, and South Africa is viewed as a suitable platform to establish a common ground and align the interests of the participating countries on five key spheres of Internet governance: infrastructure development, legal matters, economic issues, development, and social and cultural perspectives. The goal of this article is to study BRICS' approach to Internet governance. The study presents an analysis of the BRICS countries' priorities regarding Internet governance and incorporates a panel data on BRICS' commitments and decisions regarding the issue. Several conclusions on the BRICS approach to Internet governance were drawn: the most prominent sphere for BRICS cooperation is digital infrastructure development; considerable discrepancies exist among the BRICS states regarding managing Internet content that contribute to a lack of concrete decisions on social and cultural aspects of Internet governance; there is a step-by-step convergence of the BRICS counterterrorism and counter-extremism agenda with a broader issue of cybersecurity. The author assumes that the infrastructure component dominates the BRICS Internet governance discussion due to China's influence, which gives it the potential to be one of the key players and agenda-setters within BRICS, along with Russia. Steady incorporation of the counterterrorism and counter-extremism agenda into the cybersecurity discussion is strongly supported by Russia, in keeping with its declared national priorities regarding Internet governance. In the author's opinion, it would be problematic for BRICS to reach a collective decision regarding Internet content governance given the conflict of interests among the participating countries revealed by this analysis.

Introduction

The Internet, as a unique network technology, is the basis of a growing digital economy that is "that part of economic output derived solely or primarily from digital technologies with a business model based on digital goods or services" [Bukht, Heeks, 2017, p. 13]. Estimates of the digital economy's size vary from 4.5–22.5% of the global GDP depending on the selected methodology; some scholars argue that digitally developed states experience growth rates that are 1.7 times greater than the global average [Herbert, Loudon, 2020, pp. 2, 8]. Thus, the Internet and information and communications technologies (ICTs) in general can be regarded as the most important means of production today [Pozdnyakova et al., 2019].

Along with benefits, the Internet facilitates various threats due to the Internet's nature— namely its

---

[1] This article was submitted 17 January 2022

decentralized structure[2] and inhomogeneous internal "geography"[3]—which obstructs attribution of threat to states and personal digital security to a particular jurisdiction and thus impedes the ability to give new dangers a proper response [Lukackij, 2015; Verhelst, Wouters, 2020, p. 142]. The importance of countering Internet-driven threats is acknowledged at a very high level—many countries,[4] including the Russian Federation [President of the Russian Federation, 2016], have adopted information security doctrines or similar documents that prioritize cybersecurity.

The main problem within this context is the lack of a central decision-making body responsible for development of the Internet and for settling current issues related to its functionality. The international Internet governance regime is still being formed. Only a few specific technical issues, such as internet addressing,[5] usage of the domain name system (DNS), allowing networked devices to communicate, and the assignment and administration of the top-level domain system (including public domains such as ".com") can be regarded as settled [Kasenova, 2013, pp. 44–5].

As discussed in the academic literature, Internet governance is more than mere technical regulation and implies economic aspects, cybersecurity, the human rights agenda, intellectual property rights, digital taxation, and many other issues [Kurbalija, Gelbstein, 2005; Zinovieva, 2010, 2015]. Discussion and negotiations will lead to the formulation of common principles, norms, regulations, and decision-making procedures shaping the Internet's evolution and usage [Kurbalija, Gelbstein, 2005, p. 13]. It should be noted that Internet governance itself is a sub sphere of cyber domain governance [Nye, 2014], adding a vertical perspective to the issue.

Besides semantic plurality, the notion of Internet governance must take account of the involvement of actors of various types. States, while remaining the bearers of Westphalian or "classical" sovereignty,[6] when addressing issues of governing the digital realm have lost ground against professional communities responsible for standard-setting, led by the Internet Society (ISOC), international discussion platforms like the United Nations (UN) Internet Governance Forum (IGF), non-profit organizations, and other actors [Mueller, 2019; Lebedeva et al., 2016; Liaropoulos, 2013, 2016; van Horenbeeck, 2018].

Thus, one may conclude that emergence of a universal model of Internet governance is highly unlikely; it would require a high level of convergence of interest among multiple actors of different natures, pursuing their own interests [Kurbalija, Gelbstein, 2005, p. 34]. This explains why an international consensus on Internet governance issues has not been reached so far, despite the importance of the Internet to the global community. Taking into account the rapid pace of innovations, which is far ahead of the political decision-making process [OECD, 2019], an optimal way to reach consensus on Internet governance is a worthy subject for research.

The complexity of the issue hangs together with a main trend in global politics, namely a drive to polycentricity [Kuznetsov, 2020, p. 124]. The institutional basis and structure of global politics is changing rapidly, leading to emergence of new forms of international cooperation that are based on a more fair system of exchange and allocation of power; the political process itself at present is multilayered and networked [Kuznetsov, 2020, p. 124]. These tendencies elevate the influence of transregional governance bodies with club-like structures—the Group of 20 (G20) and the BRICS grouping of Brazil, Russia, India, China, and South Africa.

Why are these structures of particular interest when discussing Internet governance? The main advantage of G20/BRICS-like institutions is that they are more flexible than traditional international organizations when it comes to decision-making. The UN remains the primary platform for building international consensus on cybersecurity; however, one cannot ignore difficulties accompanying the

---

[2] This refers to the fact that there is no single decision-making body responsible for governing issues related to the global network's functionality and development. These functions are unevenly diffused among various actors including states, international organizations, professional communities, and others [Vasilkovsky, Ignatov, 2020].
[3] Of note are several papers by D. Barinova on the issue of Internet mapping and its asymmetry [2010a, 2010b, 2011].
[4] See, for example, the U.S.' Interim National Security Strategic Guidance [The White House, 2021], the EU's Cybersecurity Strategy for the Digital Decade [EU, 2021], and Korea's National Cybersecurity Strategy [Republic of Korea, 2019].
[5] The so-called system of IP addresses.
[6] When discussing Internet governance, the term "digital sovereignty" is used more often. See the review of the concept of sovereignty by S. Couture and S. Toupin [2019]

negotiation process.[7]

BRICS, as a transregional body, could serve as an effective mechanism for finding common ground on Internet governance issues and could bolster international support for it. Here are the arguments.

BRICS enjoys all the advantages of transregional governing bodies. To begin, BRICS is free from a complex bureaucracy that hampers discussion [Kuznetsov, 2020]. Against the criticism that this feature impedes practical cooperation [Cooper, Farooq, 2015; Kokotsis, 2017; Toloraya, Chukov, 2016; Toropchin, 2017], analysis of BRICS' institutionalization process gives a reason to be optimistic. Launched in 2014, the BRICS New Development Bank "represents a formal institutional extension of the BRICS as an informal club" [Cooper, Farooq, 2015, p. 36], proving its resiliency and potential to make collective decisions despite existing political and economic controversies among some of the members. Moreover, BRICS, being an "exclusive club," not only creates its own mechanisms but also exercises "catalytic influence" over other global governance institutions, stimulating or promoting shifts and reforms of international organizations [Larionova, 2016, p. 77].

Another argument in favour of BRICS derives from the results of analysis of BRICS states' performance when it comes to fulfilling the commitments made at annual summits. Their shared "understanding of the urgency for collective action" [Larionova, Rakmangulov, Shelepov, 2016, p. 89] allows for performance at a quite high average score of 74%.[8] As discussed below, BRICS' decisions on ICT development and digital growth are among those with the highest scores regarding fulfilment [Larionova et al., 2020]; for many years, the total number of commitments on this issue has been growing as well.[9]

BRICS might be considered a priority platform for discussing reform of the Internet governance system due to the current geopolitical situation and the broader context of Russia's national priorities. All BRICS members participate in G20 discussions together with global digital leaders. However, the G20 tends to follow the recommendations of the Organisation for Economic Co-operation and Development (OECD) regarding digital cooperation and development [Larionova, Shelepov, 2021, p. 43]; BRICS' influence over the OECD decision-making process is quite limited. One cannot ignore the inconsistency of Russian and U.S. positions within the UN-led negotiation process [Ibid., p. 33]. Also, it should be noted that there is a more or less comparable level of digital development among BRICS countries [Ignatov, 2020] and thus, some general communality of digital development goals.

Analysis of available literature on the subject proves the necessity of a deeper exploration. Researchers of BRICS' Internet governance often ignore the specificity of BRICS as an institution, focusing on unilateral actions of the members without explicit relation to the institution's agenda [Araújo Monteiro Neto, 2018; Belli, 2021; Galloway, 2015; Polatin-Reuben, Wright, 2014; Sokolov et al., 2017]. Other authors analyze BRICS' digital agenda, but the available examples focus on the digital economy at large without an explicit reference to Internet governance [Ignatov, 2020; Inshakova, Mitrofanova 2020; Morozkina, 2020; Tkachenko, 2018].

The present article is designed to bridge this gap. BRICS' agenda on Internet governance, and the factors that shape it, are studied through an examination of BRICS countries' strategic documents to determine their priorities regarding Internet governance and the collective decisions taken by BRICS.

The article is structured as follows: first, the issue of the Internet governance subject field, meaning

---

[7] An illustrative example is the outcome of negotiations within the UN-backed Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on cybersecurity; the latter was launched following Russia's proposal, which came after the GGE process had failed to produce any kind of a tangible result. Due to inconsistencies of Russia's and the U.S.' positions, both formats have been operating simultaneously since 2018. The U.S. favoured discussion in the closed format of the GGE; Russia invited all concerned parties to participate. Concluding reports were presented in March–May 2021 but neither the GGE nor the OEWG achieved a breakthrough; conclusions in both cases were compromises by nature and included an invitation to continue the discussion to find a long-sought consensus.

[8] This analysis draws on the University of Toronto and the Center for International Institutions Research (Moscow) joint project's results. See the BRICS Compliance Assessment [BRICS Information Centre, n.d.].

[9] Based on the panel data and the Moscow summit compliance assessment (2015–20), the share of ICT/digital economy-related decisions made by BRICS has reached 4.2% out of the total number. Russia's BRICS presidencies in 2015 and 2020 are marked with 18 and 16 decisions made on the issue, respectively; 58 decisions were made in five years in total. BRICS makes seven specific collective decisions on this issue annually.

key aspects of managing the global web that require taking multilateral actions, is discussed; then, the results of the analysis of BRICS members' Internet governance strategic priorities and BRICS' multilateral decisions on the issue, reflected in ministerial agreements and leaders' declarations, are presented.

Along with general scientific methods—content analysis, historical method, and comparative analysis—the methodology developed by the University of Toronto to study the compliance of the Group of 7 (G7), the G20, and BRICS is applied. This methodology is very important as it provides enough empirical data to deliver substantiated expert conclusions regarding the institution's agenda and prospects.[10]

Internet Governance: Setting the Subject Field

Discussion of the subject field of Internet governance is something more than "merely linguistic pedantry" [Kurbalija, Gelbstein, 2005, p. 10]. The plethora of participating actors and issues for discussion is accompanied by a broad list of potential cooperation formats and collective discussion mechanisms. A visual interpretation of this complex matter was presented for the first time by the Diplo Foundation in 2005; it is known as "The Internet Governance Cube" (Figure 1).
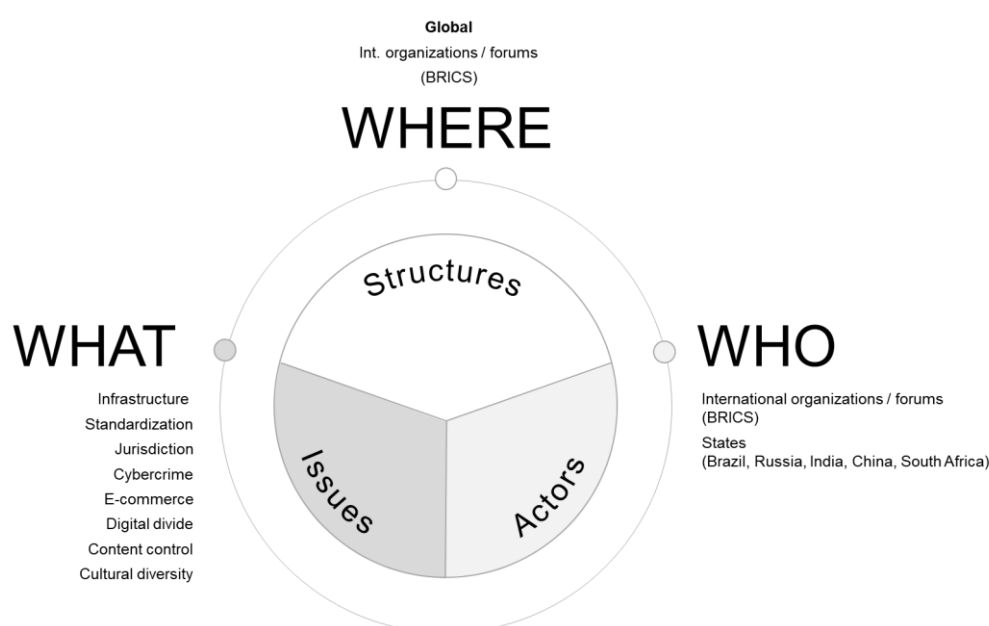

Figure 1. The Internet Governance Subject Area

Source: Prepared by the author based on J. Kurbalija and E. Gelbstein [2005].

J. Kurbalija and E. Gelbstein, the authors of the model, described it in the following way:

"The WHAT axis is related to the ISSUES of Internet Governance (for example, infrastructure, copyright, privacy). It conveys the multi-disciplinary aspect of this approach. The WHO axis of the cube focusses on the main ACTORS (states, international organizations, civil society, the private sector). This is the multistakeholder side. The WHERE axis of the cube deals with the FRAMEWORK in which Internet issues should be addressed (self-regulatory, local, national, regional, and global). This is a multi-layered approach to Internet Governance. When we move pieces in our cube we get the intersection—HOW. This is the section of the cube that can help us to see how particular issues should be regulated, both in terms of cognitive-legal techniques (e.g. analogies) and in terms of instruments (e.g. soft law, treaties, and declarations). For example, one specific intersection can help us to see HOW privacy issues (what) should be addressed by civil society (who) at the national level (where)" [2005, p. 143].

The "where" and "who" questions are already answered—the positions of Brazil, Russia, India,

---

[10] For more information on the used method see: Global Governance Program [2020].

China, and South Africa on the key issues of Internet governance are discussed below, followed by analysis of how they transform into collective BRICS decisions. The "what" axis requires further explanation.

Kurbalija and Gelbstein identify five baskets on which the Internet governance system is built—the infrastructure and standardization basket;[11] the legal basket;[12] the economic basket;[13] the development basket;[14] and the socio-cultural basket[15] [2005, p. 27]. These baskets will be used to compare BRICS members' priorities regarding Internet governance. Then, BRICS' collective decisions will be classified and analyzed following the same pattern.

BRICS Members' Declared Priorities

Analysis of the strategic documents of Brazil, Russia, India, China, and South Africa make it possible to highlight matching priorities on the above-mentioned Internet governance subject baskets.

Development of backbone digital infrastructure turned out to be a matter of mutual interest for the BRICS states (see Table 1). Some discrepancies can be explained by existing gaps regarding digital development in general; Russia and China take the lead in this regard [Ignatov, 2020]. These two countries prioritize infrastructure development in remote areas without focusing on providing better access to the poor, as India, Brazil, and South Africa do.

Another interesting case is China's attitude toward building international partnerships. Among BRICS members, it is only China that declares this to be a national priority. Implementation of infrastructure projects in Arabic countries and acceleration of the China-ASEAN Information Harbor are included in the Digital Silkroad concept. The other BRICS states are more concerned with domestic matters in this regard.

Table 1. BRICS Members' Declared Priorities on the Infrastructure Internet Governance Basket

Brazil	Russia	India	China	South Africa
Key Documents, Strategies and Programs				
Digital Transformation Strategy [Government of Brazil, 2018]; Economic and Social Development Strategy Until 2031[Government of Brazil, 2021]	National program "Digital Economy of the Russian Federation" [Government of Russia, 2019a]; Spatial Development Strategy of the Russian Federation Until 2025 [Government of Russia, 2019b]	Program "Digital India" [Government of India, 2015]; National Digital Communications Policy [Government of India, 2018]	14th Five-Year Plan [Government of China 2021a]; National strategy for informatization development for 2006–2020 [Government of China, 2006]	National Development Plan 2030 [Government of South Africa, 2012]
Priorities				

---

[11] The telecommunications infrastructure, technical standards, Internet protocol, the domain name system, root servers, Internet service providers, and the economic model for internet connectivity, among other things.

[12] Intellectual property rights, trademarks, copyrights, patents, cybercrime, labour law, and privacy and data protection, among other things.

[13] E-commerce, consumer protection, taxation, customs, e-banking, and e-money.

[14] Digital divide, universal access, and strategies for overcoming the digital divide.

[15] Content policy, human rights, multilingualism and cultural diversity, global public good, and education.

National digital infrastructure development, focus on poor and remote areas	National digital infrastructure development, focus on remote areas	National digital infrastructure development, focus on poor and remote areas	Small and middle-sized cities, rural areas digital infrastructure development, international networked projects, including the Digital Silkroad	National digital infrastructure development, focus on poor and remote areas

Among the typical issues in the legal basket of Internet governance, cybersecurity is turning out to be the most discussed topic in BRICS countries' strategic documents (see Table 2). The BRICS quintet can be divided into two groups—the Brazil-Russia-China troika and the India-South Africa duet—each pursuing different models of securing digital sovereignty—strong and weak, respectively.

S. Couture and S. Toupin reviewed the strong and the weak digital sovereignty concepts [2019]. Based their findings, the weak sovereignty concept refers to attempts by private entities to provide data security focusing on digital rights, while the strong sovereignty concept implies government policy aimed at ensuring national security.[16]

In the first case, the role of the state seems limited as data governance issues do not necessarily correspond with state security. From this point of view, there are some similarities in India's and South Africa's declared priorities. It should be mentioned that India prioritizes a user data localization agenda that may demonstrate the country's steady drive to a more explicit strong sovereignty policy.[17] The other BRICS states put forward a data localization agenda as well, but as of now India does not aim to establish centralized data and related cyber risks management systems.

Brazil, Russia, and China might be combined as strong digital sovereignty advocates. The troika values a centralized data governance model; in the case of Russia, the goal is to strengthen the country's sovereignty in the information domain following the national security strategy's wording.

BRICS' common ground in this respect is the promotion of international cooperation. Along with typical practice-oriented goals such as exchanges of good practices and capacity development, it is more active participation in the decision-making processes of the key international platforms regarding the applied standards that is shared by all BRICS members as a first-class priority. Here should be noted South Africa's focus on the African Union as a key international body to discuss and formulate multilateral decisions regarding cybersecurity.

BRICS' Internet governance agenda for the economic basket is mostly concentrated on issues related to e-commerce and digital platforms governance (see Table 3). All BRICS countries are interested in continuous growth in the volume of e-commerce; however, the partnering countries play on different fields when it comes to assessing the maturity of state policy on the matter. Brazil, Russia, and China have already passed the initial stage of formulating state policy on e-commerce and now focus on competition and the protection of users' rights on digital platforms along with building-up international partnerships to define "rules of the road." India recently announced that its national e-commerce strategy is under development; as of the time of writing, the strategy had not been finalized. With the exception of the Digital Communications Law adopted in 2005 manifesting promotion of e-payment instruments among micro, small and medium enterprises (MSMEs), analysis of South Africa's strategic documents did not show any other priorities regarding economic aspects of Internet governance.

---

[16] Couture and Toupin use the concept as explained in D. Polatin-Reuben and J. Wright [2014].

[17] See the article by A. Mukhopadhyay on developing country discourse on data localization [2020].

Table 2. BRICS Members' Declared Priorities on the Legal Internet Governance Basket

Brazil	Russia	India	China	South Africa
Key Documents, Strategies and Programs				
Cybersecurity strategy [Presidency of the Republic of Brazil, 2021a]	National security strategy of the Russian Federation [President of the Russian Federation, 2021]; "Information Security" Federal project [Government of Russia, 2019c]	National Digital Communications Policy [Government of India, 2018]	14th Five-Year Plan [Government of China, 2021a]; Personal Data protection law [Government of China, 2021b]	South Africa Cybersecurity Policy Framework [Government of South Africa, 2015]
Priorities				
National legislation adaptation; establishment of centralized cyberthreats management system; capacity building and sharing in expertise and practices	Strengthening of sovereignty in the cyber domain; cyberthreats prevention; data localization; capacity building; international cooperation on related matters	Compliance with the net neutrality principle; personal data rights; data privacy protection	Data management centralization (gathering, storage and usage); personal data online validation system improvement; transparent multilateral cybersecurity decision-making process on international fora	Cybercrime cooperation within the African Union along with regional and transregional initiatives; more active involvement in multilateral decision-making process; promotion of cybersecurity culture

Table 3. BRICS Members' Declared Priorities on the Internet Governance Economic Basket

Brazil	Russia	India	China	South Africa
Key Documents, Strategies and Programs				
Digital Transformation Strategy [Government of Brazil, 2018]	Digital Platforms and Ecosystems State Regulation Concept [Government of Russia, 2021]	Draft E-Commerce Policy [Government of India, 2019]; "Digital India" Program [Government of India, 2015]	"Internet+" Strategy [Xu, 2015]; 14th Five-Year Plan [Government of China, 2021a]; Anti-Monopoly Guidelines for the Platform Economy Industries [Government of China, 2020]; Digital renminbi White Paper [Government of China, 2021c]	Electronic Communications Act (2005) [Government of South Africa, 2005]
Priorities				
Working on international agreements on e-commerce platforms' exploitation	Exercising control over digital ecosystems	Net neutrality as digital platforms' basic working principle	Competition protection against foreign digital monopolists	E-payment instruments' proliferation among MSMEs

The development basket of BRICS' Internet governance agenda is focused on the digital infrastructure availability provision and the spread of digital skills (see Table 4). Inconsistencies found in the analysis of BRICS' strategic documents can be explained by differences in the members' digital development levels. Thus, Russia prioritizes proliferation of advanced digital skills including programming, Internet of things-based solutions, cloud computing, and so on, while Brazil, India, and South Africa, and China to some extent, are more focused on providing access to basic digital skills with a special emphasis given to rural populations and marginalized strata.

Table 4. BRICS Members' Declared Priorities on the Internet Governance Development Basket

Brazil	Russia	India	China	South Africa
Key Documents, Strategies and Programmes				

Digital Transformation Strategy [Government of Brazil, 2018]	"Personnel for the Digital Economy" Federal Project (2019–2024) [Government of Russia, 2019d]	"Digital India" Program [Government of India, 2015]	14th Five-Year Plan [Government of China, 2021a]	National Development Plan 2030 [Government of South Africa, 2012]; National Digital and Future Skills Strategy [Government of South Africa, 2020]
Priorities				
Bridging the gap in basic digital skills and digital infrastructure accessibility	Remote areas digital infrastructure development; advanced digital skills proliferation	Bridging the gap in basic digital skills and digital infrastructure accessibility	Bridging the gap in digital infrastructure accessibility	Bridging the gap in basic digital skills and digital infrastructure accessibility

Considerable differences were found in the BRICS members' positions regarding the Internet governance social-cultural issue basket (see Table 5). All BRICS countries declare adherence to human rights protection principles both online and offline, but each case is characterized by a variety of realization practices.

Among the BRICS states, Brazil and South Africa might be considered the most liberal regarding Internet materials regulation. Available assessments do not contain any tangible proof of either the Brazilian or the South African governments suppressing digital platforms or Internet users, or consistency in such attempts if there are any.[18] South Africa is the only member that puts forward promotion of cultural and language diversity while discussing Internet governance.

Russia, India, and China execute selective content control policy on the Internet. In Russia, information that is considered to violate constitutional order is strictly contained; China works to control the spread of information regarding the status of Taiwan and Tibet, the situation in Xinjiang-Yugur autonomous region, and public criticism of the Chinese government. In India, there are some limits on spreading information regarding the activities of particular religious and human rights activist groups and the spread of novel coronavirus; published in 2021, India's Intermediary Guidelines and Digital Media Ethics Code requires digital media operators to filter and delete unwarranted content within 36 hours of an official notification to do so [Republic of India, 2021].

---

[18] Published in 2021, Jair Bolsonaro's presidential order limited the right of major digital platforms to dispose or contain the spread of information circulating over the Internet without court ruling unless this information is regarded as justification of terrorism, threat of violence, sexual abuse, or cybercrime.

Brazil	Russia	India	China	South Africa
Key Documents, Strategies and Programs				
The Internet and the Digital Bill of Rights [Presidency of the Republic of Brazil, 2014]; Provisional measure No.1068 6 September 2021 [Presidency of the Republic of Brazil, 2021b]	Federal Law "On Amending "On Communications" Federal Law" 30 December 2020 [Government of Russia, 2020]; Federal Law "On Information, Information Technologies and Information Protection" [Government of Russia, 2006] Information security doctrine of the Russian Federation [President … , 2016]	Intermediary Guidelines and Digital Media Ethics Code [Government of India, 2021]	Cybersecurity Law [Government of China, 2017]; Counterterrorism Law [Government of China, 2015]	National Integrated Policy ICT White Book [Government of South Africa, 2016]
Priorities				
Provision of basic citizen rights on the Internet; democratic and transparent Internet governance	Executing strict control over Internet content to ensure constitutional order, provision of citizen rights, traditional values; building-up resilient and non-conflictual intergovernmental relations in the information sphere	Executing strict control over specific types of Internet content by establishing requirements for digital media	Executing strict control over Internet content and behaviour of Internet users	Provision of basic citizen rights on the Internet; cultural and language diversity on the Internet; democratic and transparent Internet governance

Table 5. BRICS Members' Declared Priorities on the Internet Governance Social-Cultural Basket

Thus, analysis of BRICS members' priorities on Internet governance shows that infrastructure development and overcoming the digital gap agenda are the top shared priorities. Imbalances in the BRICS countries' digital development levels explain differences in declared priorities regarding the Internet governance economic basket agenda; however, the most significant differences were found with respect to Internet content and regulation of users' behaviour.

Internet Governance in BRICS' Documents and Decisions

BRICS addressed digital development issues for the first time at the first communications ministers meeting in 2015, during Russia's second presidency. Before this, digital development had been an integral part of the broader scientific cooperation agenda [Larionova et al., 2020].

Digital development is an important topic for BRICS as indicated by the total number of commitments attributed to the ICT and digital economy sphere, to which the Internet governance agenda is connected. This issue block stands quite close to the counterterrorism, macroeconomics, regional security, trade, and development spheres that form the core BRICS agenda.

Table 6 presents the results of analysis and classification of BRICS' decisions regarding Internet governance following the Internet Governance Cube model.

Table 6. Selected Decisions and Multilateral Initiatives Taken by BRICS on Internet Governance

Baskets	Decisions (Examples)
Infrastructure	We commit ourselves to focus on expanding universal access to all forms of digital communication and to improve awareness of people in this regard (Ufa, 2015) [BRICS, 2015b] We will enhance joint BRICS research, development and innovation in ICT including the Internet of Things, Cloud computing, Big Data, Data Analytics, Nanotechnology, Artificial Intelligence and 5G and their innovative applications to elevate the level of ICT infrastructure and connectivity in our countries (Xiamen, 2017) [BRICS, 2017c] + *Terms of Reference of BRICS Model E-Port Network* [BRICS, 2017a] We will continue to take mutually beneficial initiatives in the six cooperation areas identified in the Work Plan, as agreed at the BRICS 2nd PartNIR meeting held in Brasilia in September 2019, including establishing BRICS industrial and science parks,

	innovation centers, technology business incubators and enterprises network (Brasilia, 2019) [BRICS, 2019b] [… members of BRICS will take steps to:] expand BRICS collaboration on software and ICT equipment, and realization of projects in this realm (Moscow, 2020) [BRICS, 2020b]
Legal	We will advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet that can be widely accepted by all parties concerned, and jointly build a network that is safe and secure (Xiamen, 2017) [BRICS, 2017c] We reaffirm the importance of advancing the intra-BRICS cooperation, including through the consideration of relevant initiatives and the implementation of the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs (Moscow, 2020) [BRICS, 2020b]
Economic	We will act on the basis of principles of innovation, partnership, synergy, flexibility, open and favorable business environment, trust and security, protection of consumer rights in order to ensure the conditions for a thriving and dynamic digital economy, that will foster global economic development and benefit everyone (Xiamen, 2017) [BRICS, 2017c] + *BRICS E-Commerce Cooperation Initiative* [BRICS, 2017b] [In the context of accelerated development of the e-commerce sector and increased volume of online transactions worldwide,] we will enhance our cooperation through the BRICS Ecommerce Working Group (Moscow, 2020) [BRICS, 2020b]
Development	We affirm our commitment to bridging digital and technological

	divides, in particular between developed and developing countries (Goa, 2016) [BRICS, 2016] [… members of BRICS will take steps to:] address digital divide by bridging the gap in access of BRICS population to digital infrastructure, digital skills and digitally-enabled services and ensure inclusion of digitally deprived segments of society by laying special stress on improving the access and connectivity of people living in rural areas, as well as groups of persons with disabilities, to the Internet (Moscow, 2020) [BRICS, 2020b]
Social-cultural	[… members of BRICS will take steps to:] develop digital literacy programs for harmonious and inclusive adaptation of the BRICS population (Moscow, 2020) [BRICS, 2020b]

The most developed Internet governance basket within the BRICS agenda is infrastructure development. Almost every presidency has resulted in a concrete, implicit collective decision on network development. China's second presidency (2017) and Russia's second and third presidencies (2015 and 2020, respectively) can be seen as turning points in this regard.

Some of the collective BRICS decisions are worth further explanation.

The first BRICS collective decisions on Internet governance were the ICT Development Agenda and the Action Plan adopted in 2016 during India's presidency [BRICS Working Group on ICT Cooperation, 2016]. The agenda and plan elaborate concepts expressed at the first communication ministers meeting in Moscow in 2015, resulted with the joint Communique "Expansion of Cooperation in the Field of Communications and ICTs" [BRICS, 2015a].

At that meeting, the BRICS communication ministers addressed a wide range of issues, namely existing development gaps and software distribution, global market diversification, bridging global digital inequality (emphasizing developing countries), and respect for human rights. For the first time, BRICS countries expressed the importance of the "establishment of mechanism for the Internet governance based on the principles of multilateralism, democracy, transparency and mutual trust" and highlighted "the sovereign rights of States to participate in governing the Internet in their respective jurisdictions in accordance with international law and the adherence to fundamental human rights and freedoms."

The agenda and plan based on the above-mentioned communiqué [BRICS, 2015a] include the establishment of the special BRICS Working Group—the track two BRICS ICT cooperation

format. The 2016 plan prioritized an "open and secure" Internet and noted that "states should participate on an equal footing involving relevant stakeholders in respective roles and responsibilities."

In 2017, during China's second presidency, BRICS agreed on two major initiatives—the Terms of Reference of BRICS Model E-Port Network and the BRICS E-Commerce Cooperation Initiative. The first focused on the practical implementation of ICT in logistics, maritime infrastructure management, and trade, while the latter aimed to establish a designated working group, better communications with the BRICS business community, and joint research to facilitate eradication of trade barriers.

South Africa's 2018 BRICS presidency did not bring much to the table regarding digital development and Internet governance. However, in Johannesburg, the leaders agreed to establish the Partnership on New Industrial Revolution (PartNIR) designed as a platform facilitating networking and sharing best practices, including in ICTs [BRICS, 2018].

In 2019, with Brazil as host, the BRICS communication ministers adopted a joint declaration [BRICS, 2019a] dedicated to issues bordering the infrastructure and social-cultural baskets. The ministers called for better access to broadband communications to facilitate inclusive growth and sustainable development and highlighted the importance of digital skills proliferation and the education systems and labor market's adjustment to digital transformation. Digital security was discussed from an unusual point of view as relating to more equal distribution of digital growth benefits while providing reliable means of protection against emerging digital threats.

Russia's 2020 BRICS-Shanghai Cooperation Organization presidency marked a long-term trend of shifting BRICS' Internet governance agenda from infrastructure and economic issues to the legal basket with a special emphasis on security. In Moscow, BRICS states adopted the Counter-Terrorism Strategy [BRICS, 2020a], which highlighted the goal of combatting "extremist narratives conducive to terrorism and the misuse of the Internet and social media for the purposes of terrorist recruitment." The word "Internet" was mentioned three times in the Moscow leaders' declaration: for the first time, the leaders addressed the issue of countering extremist material spreading on the Internet, and in two other cases in relation to protecting children against illicit content and online activities "harmful for their health and development."

India's 2021 BRICS presidency secured the trend toward deeper online security cooperation. In New Delhi, the BRICS leaders adopted the Counter Terrorism Action Plan [BRICS, 2021] that recalled BRICS' decisions on containing the spread of extremist and terrorist narratives, propaganda, and terrorist groups' recruiting activities. During the summit, the leaders discussed the overview of BRICS' best practices on online financial safety. In the concluding declaration the leaders expressed concerns over "increasing challenge to protect children from online sexual

exploitation and from other content harmful for their health and development" and highlighted the urgent need for active cooperation among BRICS states on countering terrorist content on the Internet.

Conclusion

In a relatively short period of time, from 2015–21, BRICS fulfilled collective commitments on Internet governance issues. Russia's and China's presidencies are marked with the most active discussions and decision-making processes. Analysis of BRICS' Internet governance agenda and BRICS countries' strategic priorities, collective decisions, and joint initiatives in this regard leads to the following conclusions.

Quantitative analysis of BRICS' Internet governance decisions shows that, among the five key baskets, the infrastructure and economic components are the most prominent. China has been actively promoting further discussions on issues related to digital infrastructure development. Despite the fact that BRICS has transformed from a loosely connected group of fast-growing economies into a multifaceted discussion platform [Kuznetsov, 2020, pp. 126–7; Larionova et al., 2020], economic cooperation issues remain the top priority. China has launched a plethora of collective initiatives on digital infrastructure development that match the country's declared development priorities. BRICS partners generally act in favour of China's proposals. One may expect that China's 2022 BRICS presidency will give the infrastructure development agenda proper attention, resulting in a series of collective decisions.

 Another interesting observation regarding BRICS' Internet governance agenda is the growing importance of security-related issues, with a special emphasis on cybersecurity within the broader context of counterterrorism and extremism policy. Among the BRICS states, it is Russia that favours multilateral discussion on the matter; the partnering countries welcome such an initiative, as is shown by the analysis of BRICS' compliance. However, in contrast to the infrastructure basket, the BRICS countries' approaches to cybersecurity are diverse to a considerable extent, and that could become an obstacle. This complex matter is beyond the scope of this article and requires further exploration.

The other Internet governance issues—e-commerce, development, and social-cultural matters—are presented in the BRICS agenda but draw much less attention. In practice, these have been the subject of a relatively limited number of commitments and collective decisions. The essence of decisions made on these matters should also be taken into account—for instance, the development basket overlaps with the digital infrastructure component so broadly that it is somehow overshadowed by it, such that the two could be folded into one.

Analysis of the BRICS agenda also shows that the widest gap among the partner countries lies in the social-cultural Internet governance basket. The complexity of the decision-making process

resulted in quite a few collective decisions that were defined by the existing diversities among the BRICS states regarding the practical realization of human rights both offline and online. To make it work, two major actors—Russia and China—must change their attitude; as of now, they prioritize cooperation in other spheres.

References

Araújo Monteiro Neto J. (2018) The Operation of Multistakeholderism in Brazilian Internet Governance: Governance Innovation Through Multistakeholderism Generativity. Unpublished PhD Dissertation, University of Kent. Available at: https://kar.kent.ac.uk/76961/ (accessed 2 June 2022).

Barinova D. S. (2010a) Nacional'nye domeny interneta - simvoly gosudarstvennyh granic i bezgranichnyh vozmozhnostej [National Top-Level Domains: Symbols of State Borders and of Borderless Possibilities]. *MGIMO Review of International Relations*, no 5(14), pp. 307–14. Available at: https://doi.org/10.24833/2071-8160-2010-5-14-307-314 (in Russian).

Barinova D. S. (2010b) Metodologicheskie aspekty issledovanija virtual'nogo prostranstva Interneta [Methodological Aspects of Studying the Internet Virtual Realm]. *Metod*, no 1, pp. 109–22 (in Russian).

Barinova D. S. (2011) Asimmetrija Virtual'nogo Politicheskogo Prostranstva. Rezul"taty Sravnitel'nogo Analiza Dannyh 255 Nacional"nyh Domenov Interneta [Asymmetry of the Virtual Political Space: Results of the Comparative Analysis of the Data of 255 National Internet Domains]. *Comparative Politics Russia*, vol. 2, no 4(6), pp. 13–8. Available at: https://doi.org/10.18611/2221-3279-2011-2-4(6)-13-18 (in Russian).

Belli L. (ed) (2021) *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*. Springer Cham. Available at: https://doi.org/10.1007/978-3-030-56405-6.

BRICS (2015a) Meeting of the BRICS Communications Ministers. Moscow, 22–23 October. Available at: http://en.brics2015.ru/program/20151022/539909.html (accessed 31 March 2022).

BRICS (2015b) VII Summit Ufa Declaration. Available at: https://www.ranepa.ru/images/media/brics/ruspresidency2/Declaration_eng.pdf (accessed: 12 July 2022)

BRICS (2016) Goa Declaration. Available at: https://www.ranepa.ru/images/media/brics/indianpresidency2/Goa%20Declaration.pdf (accessed: 12 July 2022)

BRICS (2017a) Terms of Reference (ToR) of BRICS Model E-Port Network (Final Version). Available at: https://www.ranepa.ru/images/media/brics/china2016/ToR%20of%20BRICS%20Model%20E-Port%20Network%20-%20Final.pdf (accessed 31 March 2022).

BRICS (2017b) E-Commerce Cooperation Initiative (Final Version). Available at: https://www.ranepa.ru/images/media/brics/china2016/BRICS%20E-commerce%20Cooperation%20Initiative_final%20(2).pdf (accessed 31 March 2022).

BRICS (2017c) BRICS Leaders Xiamen Declaration. Available at: https://www.ranepa.ru/images/media/brics/2017/mEsqRkedzqYLDwxo6AbZnCkmAo9Xta3d.pdf (accessed: 12 July 2022)

BRICS (2018) Johannesburg Declaration. Johannesburg, 26 July. Available at: https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration (accessed 31 March 2022).

BRICS (2019a) Declaration of the 5th BRICS Communications Ministers Meeting. Brasilia, 14 August. Available at: https://www.ranepa.ru/eng/images/CIIR/BRICS/2019/Declaration_of_the_5th_BRICS_Communications_Ministers_Meeting-_Bras%C3%ADlia.pdf (accessed 31 March 2022).

BRICS (2019b) 11th BRICS Summit – Brasilia Declaration. Available at: https://www.ranepa.ru/images/News_ciir/Project/BRICS_new_downloadings/2019/11th_BRICS_Summit_eng.pdf (accessed: 12 July 2022)

BRICS (2020a) BRICS Counter-Terrorism Strategy. Available at: https://eng.brics-russia2020.ru/images/114/81/1148168.pdf (accessed 31 March 2022).

BRICS (2020b) XII BRICS Summit Moscow Declaration. Available at: https://www.ranepa.ru/ciir/briks/predsedatelstva/briks-rossijskoe-predsedatelstvo-2020/XII%20BRICS%20Summit%20Moscow%20Declaration.pdf (accessed: 12 July 2022)

BRICS (2021) BRICS Counter Terrorism Action Plan. Available at: https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-52.pdf (accessed 31 March 2022).

BRICS Information Centre (n.d.) BRICS Compliance Assessments. University of Toronto. Available at: http://www.brics.utoronto.ca/compliance/index.html (accessed 17 March 2022).

BRICS Working Group on ICT Cooperation (2016) ICT Development Agenda and Action Plan. Available at: https://dot.gov.in/sites/default/files/11-11-2016%20BRICS%20ICT%20Development%20Agenda%20%26%20Action%20plan.pdf?download=1 (accessed 31 March 2022).

Bukht R., Heeks R. (2017) Defining, Conceptualising and Measuring the Digital Economy. Development Informatics World Paper No 68, Centre for Development Informatics. Available at: https://diodeweb.files.wordpress.com/2017/08/diwkppr68-diode.pdf (accessed 10 March 2022).

Couture S., Toupin S. (2019) What Does the Notion of "Sovereignty" Mean When Referring to the Digital? *New Media & Society*, vol. 21, no 10, pp. 2305–22. Available at: https://doi.org/10.1177%2F1461444819865984.

Cooper A. F., Farooq A. B. (2015) Testing the Club Dynamics of the BRICS: The New Development Bank From Conception to Establishment. *International Organisations Research Journal*, vol. 10, no 2, pp. 39–58. Available at: https://doi.org/10.17323/1996-7845-2015-02-39.

European Union (EU) (2020) The EU's Cybersecurity Strategy for the Digital Decade. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (accessed 31 March 2022).

Galloway T. (2015) China & Technical Global Internet Governance: From Norm-Taker to Norm-Maker? Unpublished PhD Dissertation, Deakin University. Available at: https://dro.deakin.edu.au/eserv/DU:30083119/galloway-chinaand-2015A.pdf (accessed 2 June 2022).

Government of Brazil (2018) Brazilian Digital Transformation strategy. Available at: https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/digitalstrategy.pdf (accessed: 12 July 2022)

Government of Brazil (2021) Estratégia Nacional de Desenvolvimento Econômico e Social Sumário Executivo. Available at:

https://www.platformchinaplp.mo/attachment/file/20210513/20210513181654262806.pdf
(accessed: 12 July 2022)

Government of Russia (2006) Zakon ob informacii, informacionnyh tehnologijah i zashhite informacii [Federal Law "On Information, Information Technologies and Information Protection"]. Available at: https://rg.ru/documents/2006/07/29/informacia-dok.html (accessed: 12 July 2022) (in Russian)

Government of Russia (2019a) Pasport nacional'noj programmy "Cifrovaja jekonomika Rossijskoj Federacii" [Outline of the National program "Digital Economy of the Russian Federation"]. Available at:

http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf
(accessed: 12 July 2022) (in Russian)

Government of Russia (2019b) Strategija prostranstvennogo razvitija Rossijskoj Federacii na period do 2025 goda [Spatial Development Strategy of the Russian Federation Until 2025]. Available at: http://static.government.ru/media/files/UVAlqUtT08o60RktoOXl22JjAe7irNxc.pdf
(accessed: 12 July 2022) (in Russian)

Government of Russia (2019c) Pasport federal'nogo proekta "Informacionnaja bezopasnost'" [Outline of the federal project "Information security"]. Available at:
https://digital.ac.gov.ru/poleznaya-
informaciya/material/%D0%9F%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82-
%D1%84%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0
%BE%D0%B3%D0%BE-
%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B0-
%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0
%BE%D0%BD%D0%BD%D0%B0%D1%8F-
%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1
%81%D1%82%D1%8C.pdf (accessed: 12 July 2022) (in Russian)

Government of Russia (2019d) Pasport federal'nogo proekta "Kadry dlja cifrovoj jekonomiki" ["Personnel for the Digital Economy" Federal Project]. Available at:
https://digital.ac.gov.ru/poleznaya-
informaciya/material/%D0%9F%D0%B0%D1%81%D0%BF%D0%BE%D1%80%D1%82-
%D1%84%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D0%BB%D1%8C%D0%BD%D0
%BE%D0%B3%D0%BE-
%D0%BF%D1%80%D0%BE%D0%B5%D0%BA%D1%82%D0%B0-
%D0%9A%D0%B0%D0%B4%D1%80%D1%8B-%D0%B4%D0%BB%D1%8F-
%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9-

%D1%8D%D0%BA%D0%BE%D0%BD%D0%BE%D0%BC%D0%B8%D0%BA%D0%B8.pdf (accessed: 12 July 2022) (in Russian)

Government of Russia (2020) Federal'nyj zakon ot 30 dekabrja 2020 g. N 533-FZ "O vnesenii izmenenij v Federal'nyj zakon "O svjazi"" [Federal Law "On Amending "On Communications" Federal Law" 30 December 2020]. Available at: https://rg.ru/documents/2021/01/11/svyaz-dok.html (accessed: 12 July 2022) (in Russian)

Government of Russia (2021) Koncepcija obshhego regulirovanija dejatel'nosti grupp kompanij, razvivajushhih razlichnye cifrovye servisy na baze odnoj «jekosistemy» [Digital Platforms and Ecosystems State Regulation Concept]. Available at: https://www.garant.ru/products/ipo/prime/doc/400731439/ (accessed: 12 July 2022) (in Russian)

Government of India (2015) Digital India. Available at: https://www.meity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf (accessed: 12 July 2022)

Government of India (2018) National Digital Communications Policy. Available at: https://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf (accessed: 12 July 2022)

Government of India (2019) Draft National e-Commerce Policy. Available at: https://dpiit.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf (accessed: 12 July 2022)

Government of India (2021) Intermediary Guidelines and Digital Media Ethics Code. Available at: https://transformingindia.mygov.in/wp-content/uploads/2021/02/IT-Intermediary-Guidelines.pdf (accessed: 12 July 2022)

Government of China (2006) Outline of the National Informatization Development Strategy. Available at: https://chinacopyrightandmedia.wordpress.com/2016/07/27/outline-of-the-national-informatization-development-strategy/ (accessed: 12 July 2022)

Government of China (2015) Counterterrorism Law of the People's Republic of China. Available at:

https://www.pkulaw.com/en_law/f694f0bd49b816eabdfb.html?keyword=Counterterrorism%20Law%20of%20the%20People%27s%20Republic%20of%20China (accessed: 12 July 2022)

Government of China (2017) Cybersecurity Law. Available at: https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (accessed: 12 July 2022)

Government of China (2020) Anti-Monopoly Guidelines for the Platform Economy Industries. Available at: https://www.anjielaw.com/en/uploads/soft/210224/1-210224112247.pdf (accessed: 12 July 2022)

Government of China (2021a) The outline of the 14th Five-Year Plan for Economic and Social Development and long-range objectives through the year 2035 of the People's Republic of China.

Available at: https://en.ndrc.gov.cn/policies/202203/P020220315511326748336.pdf (accessed: 12 July 2022)

Government of China (2021b) The PRC Personal Information Protection Law. Available at: https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/ (accessed: 12 July 2022)

Government of China (2021c) Zhōngguó shùzì rénmínbì de yánfā jìnzhǎn báipíshū [Research and development progress of China's digital renminbi White Paper]. Available at: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4293590/2021071614200022055.pdf (accessed: 12 July 2022) (in Chinese)

Government of South Africa (2005) Electronic Communications Act. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/a36-050.pdf (accessed: 12 July 2022)

Government of South Africa (2012) National Development Plan 2030. Available at: https://www.gov.za/sites/default/files/gcis_document/201409/ndp-2030-our-future-make-it-workr.pdf (accessed: 12 July 2022)

Government of South Africa (2015) The National Cybersecurity Policy. Available at: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf (accessed: 12 July 2022)

Government of South Africa (2016) National Integrated Policy ICT White Book. Available at: https://www.dtps.gov.za/images/phocagallery/Popular_Topic_Pictures/National_Integrated_ICT_Policy_White.pdf (accessed: 12 July 2022)

Government of South Africa (2020) National Digital and Future Skills Strategy. Available at: https://www.gov.za/sites/default/files/gcis_document/202009/43730gen513.pdf (accessed: 12 July 2022)

Global Governance Program (2020) Compliance Coding Manual for International Institutional Commitments. University of Toronto. Available at: http://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf (accessed 14 September 2022).

Herbert G., Loudon L. (2020) The Size and Growth Potential of the Digital Economy in ODA-Eligible Countries. Helpdesk Report, K4D. Available at: https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/15963/915_size_and_growth_potential_of_the_digital_economy_in_ODA-eligible_countries.pdf?sequence=1&isAllowed=y (accessed 10 March 2022).

Inshakova I., Mitrofanova I. (2020) Razvitie Cifrovoj Jekonomiki Stran Briks: Sostojanie I Prioritety [Development of the Digital Economy in the BRICS Countries: Status and Priorities].

Economics: Yesterday, Today and Tomorrow, vol. 10, no 2-1, pp. 332–48 (in Russian). Available at: http://publishing-vak.ru/file/archive-economy-2020-2/33-inshakova.pdf (accessed 18 July 2022).

Ignatov A. (2020) The Digital Economy of BRICS: Prospects for Multilateral Cooperation. *International Organisations Research Journal*, vol. 15, no 1, pp. 31–62. Available at: http://doi.org/10.17323/1996-7845-2020-01-02.

Kasenova M. (2013) Global'noe upravlenie Internetom v kontekste sovremennogo mezhdunarodnogo prava [Global Internet Governance and the International Law]. *Indeks bezopasnosti*, vol. 19, no 1(104), pp. 43–64 (in Russian).

Kokotsis E. (2017) G20 and BRICS: Enhancing Delivery Legitimacy. *International Organisations Research Journal*, vol. 12, no 2, pp. 195–211. Available at: https://doi.org/10.17323/1996-7845-2017-02-195.

Kurbalija J., Gelbstein E. (2005) Internet Governance: Issues, Actors and Divides. Diplo Foundation.

Kuznetsov D. A. (2020) Setevaja Tekstura Mirovoj Politiki: Transregionalizm Briks [Network Texture of World Politics: Transregionalism of BRICS]. *World Economy and International Relations,* vol. 64, no 11, pp. 124–31. Available at: https://doi.org/10.20542/0131-2227-2020-64-11-124-131 (in Russian).

Larionova M. V. (2016) Evaluating Global Institutions' Effectiveness. *International Organisations Research Journal*, vol. 11, no 1, pp. 69–85. Available at: https://doi.org/10.17323/1996-7845/2016-01-126.

Larionova M. V., Rakmangulov M. R., Shelepov A. V. (2016) Explaining G20 and BRICS Compliance. *International Organisations Research Journal*, vol. 11, no 2, pp. 86–111. Available at: https://doi.org/10.17323/1996-7845-2016-03-99.

Larionova M. V., Ignatov A. A., Popova I. M., Sakharov A. G., Shelepov A. V. (2020) Desjat' let BRIKS. Chto dal'she? [*BRICS at Ten: The Way Forward*]. Moscow: RANEPA (in Russian).

Larionova M., Shelepov A. (2021) Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance. *International Organisations Research Journal*, vol. 16, no 1, pp. 29–63. Available at: https://doi.org/10.17323/1996-7845-2021-01-02.

Lebedeva M. M., Kharkevich M. V., Zinovieva E. S., Koposova E. N. (2016) Arhaizacija Gosudarstva: Rol'' Sovremennyh Informacionnyh Tehnologij [State Archaization: The Role of Information Technologies]. *Polis: Political Studies*, no 6, pp. 22–36. Available at: https://www.politstudies.ru/files/File/2016/6/Polis_06_2016-Lebedeva_Kharkevich_Zinovieva_Koposova.pdf (accessed: 7 June 2022) (in Russian).

Lukackij A. V. (2015) Opredelenie istochnika kiberatak [Tracking Sources of Cyberattacks]. *Pul's*

kibermira, no 2(14). Available at: http://pircenter.org/media/content/files/13/14303840060.pdf (accessed 10 March 2022) (in Russian).

Liaropoulos A. (2013) Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction? *Journal of Information Warfare*, vol. 12, no 2, pp. 19–26. Available at: https://www.jstor.org/stable/26486852.

Liaropoulos A. (2016) Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics. *Journal of Information Warfare*, vol. 15, no 4, pp. 14–26. Available at: https://www.jstor.org/stable/26487548.

Nye J. S. (2014) The Regime Complex for Managing Global Cyber Activities. CIGI Paper Series No 1, Global Commission on Internet Governance. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (accessed 2 June 2022).

Morozkina A. (2020) Regional Perspective of Digitalization in BRICS. *International Organisations Research Journal*, vol. 15, no 4, pp. 70–90. Available at: https://doi.org/10.17323/1996-7845-2020-04-04.

Mueller L. M. (2019) Against Sovereignty in Cyberspace. *International Studies Review*, vol. 22, no 4, pp. 779–801. Available at: https://doi.org/10.1093/isr/viz044.

Mukhopadhyay A. (2020) E-commerce Trade and Data Localization: A Developing Country Perspective. *International Organisations Research Journal*, vol. 15, no 3, pp. 153–75. Available at: https://doi.org/10.17323/1996-7845-2020-03-06.

Organisation for Economic Co-operation and Development (OECD) (2019) Vectors of Digital Transformation. OECD Digital Economy Paper No 273. Available at: https://doi.org/10.1787/5ade2bba-en.

Pozdnyakova U., Mukhomorova I., Golikov V., Sazonov S., Pleshakov G. (2019) Internet of Things as a New Factor of Production in the Conditions of Digital Economy. *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT* (E. Popkova (ed)). Spring Cham. Available at: http://dx.doi.org/10.1007/978-3-030-13397-9_117.

Polatin-Reuben D., Wright J. (2014) An Internet With BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. Presented at the 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, 18 August. Available at: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben (accessed 2 June 2022).

President of the Russian Federation (2016) Ukaz Prezidenta Rossijskoj Federacii ot 05.12.2016 g. № 646 Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii [Presidential Decree No. 646 5 December 2016 "Information Security Doctrine of the Russian Federation]. Available at: http://kremlin.ru/acts/bank/41460 (accessed: 12 July 2022)

President of the Russian Federation (2021) Ukaz Prezidenta Rossijskoj Federacii ot 02.07.2021 g. № 400 O Strategii nacional'noj bezopasnosti Rossijskoj Federacii [Presidential Decree No. 400 2 July 2021 "National security strategy of the Russian Federation"]. Available at: http://www.kremlin.ru/acts/bank/47046 (accessed: 12 July 2022) (in Russian)

Presidency of the Republic of Brazil (2014) LEI Nº 12.965, DE 23 DE ABRIL DE 2014 [LAW No. 12,965, OF April 23, 2014]. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm (accessed: 12 July 2022) (in Portuguese)

Presidency of the Republic of Brazil (2021a) DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020. Available at: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm (accessed: 12 July 2022) (in Portuguese)

Presidency of the Republic of Brazil (2021b) MEDIDA PROVISÓRIA Nº 1.068, DE 6 DE SETEMBRO DE 2021 [Provisional measure No.1068 6 September 2021]. Available at: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.068-de-6-de-setembro-de-2021-343277275 (accessed: 12 July 2022) (in Portuguese)

President of the Russian Federation (RF) (2020) Ukaz Prezidenta Rossijskoj Federacii ot 27 July 2020 g. No 474 "O nacional'nyh celjah razvitija Rossijskoj Federacii na period do 2030 goda" [Decree of the President of the Russian Federation of 21 July 2020 No 474 "On the National Development Goals of the Russian Federation for the Period Up to 2030]. Available at: http://www.kremlin.ru/acts/bank/45726 (accessed 2 June 2022) (in Russian).

Republic of India (2021) Ministry of Electronics and Information Technology Notification. New Delhi, 25 February. Available at: https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf (accessed 31 March 2022).

Republic of Korea (2019) National Cybersecurity Strategy. Available at: https://ccdcoe.org/uploads/2018/10/South-Korea_English-National-Cybersecurity-Strategy-03-April-2019_English-1.pdf (accessed 14 March 2022).

Sokolov A., Shashnov S., Kotsemir M., Grebenyuk A. (2017) Identification of Priorities for S&T Cooperation of BRICS Countries. *International Organisations Research Journal*, vol. 12, no 4, pp. 32–67 (in Russian and English). Available at: https://doi.org/10.17323/1996-7845-2017-04-32.

The White House (2021) Interim National Security Strategic Guidance. Available at: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf (accessed 14 March 2022).

Tkachenko I. (2018) Perspektivy sotrudnichestva stran BRIKS v razvitii cifrovoj jekonomiki [The

BRICS Perspective on Digital Economy Development Cooperation]. *Bolshaya Evrasia: Rasvitie, Bezopsnost', Sotrudnichestvo.* pp. 339–43.

Toloraya G., Chukov R. (2016) BRICS to Be Considered? *International Organisations Research Journal*, vol. 11, no 2, pp. 97–112. Available at: https://doi.org/10.17323/1996-7845-2016-02-97.

Toropchin G. (2017) Ot Goa do Sjamjenja. O nekotoryh aspektah politicheskogo sotrudnichestva v ramkah BRIKS [From Goa to Xiamen: On Some Aspects of Political Cooperation Within BRICS]. *International Organisations Research Journal*, vol. 12, no 1, pp. 174–88. Available at: https://doi.org/10.17323/1996-7845-2017-01-174 (in Russian).

Vasilkovsky S., Ignatov A. (2020) Internet Governance: System Imbalances and Ways to Resolve Them. *International Organisations Research Journal*, vol. 15, no 4, pp. 7–29. Available at: http://doi.org/10.17323/1996-7845-2020-04-01.

van Horenbeeck M. (2018) The Future of Internet Governance and Cyber-Security. *Computer Fraud & Security*, no 5, pp. 6–8. Available at: http://dx.doi.org/10.1016/S1361-3723(18)30042-3.

Verhelst A., Wouters J. (2020) Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. *International Organisations Research Journal*, vol. 15, no 2, pp. 105–24. Available at: https://doi.org/10.17323/1996-7845-2020-02-07.

Xu, B. (2015) China Internet Plus Strategy. Available at: https://www.sesec.eu/app/uploads/2015/06/2015_05_SESECIII_Newsletter_April_2015_Annex 02_China_Internet_Plus_Strat....pdf (accessed: 12 July 2022)

Zinovieva E. S. (2010) Mezhdunarodnoe Upravlenie Internetom: Problemy, Podhody, Perspektivy [International Internet Governance: Problems, Approaches, Perspectives]. *MGIMO Review of International Relations*, no 6(15), pp. 167–74. (in Russian).

Zinovieva E. S. (2015) Global'noe Upravlenie Internetom: Rossijskij Podhod I Mezhdunarodnaja Praktika [Global Internet Governance: Russian Approach and International Practice]. *MGIMO Review of International Relations*, no 4(43), pp. 111–8. Available at: https://doi.org/10.24833/2071-8160-2015-4-43-111-118 (in Russian).