ARTICLES

THE LEVEL OF CYBERSECURITY OF THE BRICS MEMBER COUNTRIES IN INTERNATIONAL RATINGS: PROSPECTS FOR COOPERATION

OKSANA OVCHINNIKOVA,

South Ural State University (National Research University) (Chelyabinsk, Russia)

NITEESH KUMAR UPADHYAY,

Symbiosis Law School, Noida Campus (Symbiosis International Deemed University, Pune, India)

https://doi.org/10.21684/2412-2343-2023-10-1-7-34

Creating a legal framework for cybersecurity is a key factor in the digitalization of an economy. The interaction between the BRICS member countries has undergone a digital transformation, which has improved their ability to work together economically and strengthened the growing influence of these countries in the international arena. The purpose of the present study is to determine the potential of the BRICS member nations to form a joint cybersecurity strategy. The authors put forward a hypothesis that the formation of an effective cybersecurity system is possible only with a sufficient level of development of information and communication technologies and a high degree of digitalization of interstate governance. The scientific novelty of this research lies in its complex approach to the scientific and theoretical analysis of the problems of ensuring cybersecurity in the BRICS member countries, on the basis of which it identifies the common areas for cooperation. The research methodology is based on establishing a correlation between the indicators of e-government development and the criteria for state cybersecurity, followed by a comparative analysis. As a quantitative indicator, the authors use the data of the E-Government Development Index for the BRICS member countries from 2010 to 2018. Additionally, the level of maturity of each country's national cybersecurity system is reflected in the rating of the International Telecommunication Union (ITU). Based on the ITU rating, we assess the cybersecurity efficiency of the BRICS member countries versus other countries. The findings of the research lead the authors to the conclusion that state control over cyberspace and the availability of a national strategy are prerequisites for achieving a high level of cybersecurity.

Keywords: national security; cybersecurity; cyberthreats; cyberattack; information infrastructure; cyber terrorism; BRICS.

Recommended citation: Oksana Ovchinnikova & Niteesh Kumar Upadhyay, *The Level of Cybersecurity of the BRICS Member Countries in International Ratings: Prospects for Cooperation*, 10(1) BRICS Law Journal 7–34 (2023).

Table of Contents

Introduction

Cybersecurity is a critical area of global regulatory interest.[1] States seek to preserve their access to and safeguard their dependence on cyberspace, which frequently entails a departure from set norms.[2] Since 2002, the United Nations has adopted several resolutions aimed at the creation of a global cybersecurity culture.[3] However, there are still no international law institutions in place to ensure the appropriate control. This has led to competition between the states for priority in this area. The national digital economic infrastructures of the BRICS member countries have a leading position in global e-commerce. China dominates with a turnover of $2.09 trillion, while India is the fastest growing market.[4] An increase in the share of digital transactions between the BRICS member countries will allow them to significantly increase sales turnover and neutralize the disadvantages of their fragmented geographical location. Unifying

[1] Dimitra Markopoulou et al., *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, 35(6) Computer L. & Security Rev. 1 (2019).

[2] Pallavi Khanna, *State Sovereignty and Self-Defence in Cyberspace*, 5(4) BRICS L.J. 139 (2018).

[3] UN, *Creation of a Global Culture of Cybersecurity: Resolution/adopted by the General Assembly*, United Nations Digital Library System, 31 January 2003 (Feb. 2, 2023), available at https://digitallibrary.un.org/record/482184?ln=en.

[4] Global Ecommerce 2020, *Ecommerce Decelerates amid Global Retail Contraction but Remains a Bright Spot*, Report by Ethan Cramer-Flood, 22 June 2020 (Feb. 2, 2023), available at https://www.emarketer.com/content/global-ecommerce-2020#page-report.

the BRICS member countries would result in an increase in the power of the overall international system. By 2020, the total GDP of the BRICS member countries amounted to 25% of the global GDP ($21 trillion), and their share in the international commodity turnover amounted to almost 20% ($6.7 trillion). Mutual exports of the countries of 'the five' grew by 45% (from 2015 to 2019).

The focus on the digitalization of economic interaction, despite its potential advantages, is linked with certain risks. An increase in the number of operations in cyberspace inevitably leads to an increase in security threats and incidents. Cases of unauthorized penetration into the digital infrastructure of governments and businesses cannot be prevented through technological methods. They elicit a major public response in the mass media and on the Internet. The transnational nature of cyberattacks leads to the appearance of tensions between states, which in turn give rise to the need to ensure security in cyberspace by legal means.

The national policy of a state can be defined and institutionalized in cyberspace through the adoption of a cybersecurity strategy. The components of an effective cybersecurity strategy are not universal. They are determined by the extent to which the information and communications technology (ICT) of a state has developed, as well as by the peculiarities of its international and domestic policies and its management practices.[5] Cybersecurity strategy also largely depends on the proportion of the population using ICT tools in their day-to-day life.

Researchers have been actively exploring the cybersecurity strategies of developed countries, which ensure the exchange of positive experience and advanced development. Cybersecurity is defined as a means not only of protecting and defending society and its essential information infrastructures but also a way of prosecuting national and international policies through the means of information technology means.[6] According to numerous industry experts, a state's ability to prevent fundamental cyberthreats and develop a national cyber protection policy directly depends on the development level of the infrastructure meeting the requirements of international cybersecurity indices.[7] A number of countries also have their own response teams for potential cyberattacks, for example in India The purpose of the computer emergency response team is to protect and prevent any kind of cyberattacks on Indian computer system, computer network and computer resources.[8] There is an interrelation between the legal framework and the formation of cyberattack response authorities:

[5] Guide to Developing a National Cybersecurity Strategy (2018) (Feb. 2, 2023), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

[6] Tim Stevens, *Global Cybersecurity: New Directions in Theory and Methods*, 6(2) Pols. & Governance 1 (2018).

[7] Olga Vakulyk et al., *Cybersecurity as a Component of the National Security of the State*, 9(3) J. Security & Sustainability Issues 775 (2020).

[8] The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules (2013) (Feb. 2, 2023), available at https://www.meity.gov.in/writereaddata/files/G_S_R%2020%20%28E%292_0.pdf.

Cybersecurity breaches cannot be contained within the borders of a single country. Cyberattacks are launched in cyberspace, the actual boundaries of which cannot be determined.[9] When it comes to cybersecurity, the issue of jurisdiction raises serious concerns and calls for improved international cooperation in the development of a legal, technical and judicial system.

All of the BRICS member countries are considered developing countries.

> However, the BRICS association is gradually going beyond the scope of only economic cooperation and acquiring the features of institutionalization of supranational education. The logic of the stages of the unification of the BRICS member nations demonstrates rapprochement in various areas of interstate cooperation.[10]

Nevertheless, some scholars believe that in forming cybersecurity strategies, states strive to increase cyber training both in defense and offense, viewing these strategies as a new opportunity to develop their military potential.[11] To this end, the strengthening of cooperation between the BRICS member countries is limited by various types of government control that foster mutual distrust and asymmetry of power within the group.[12] In the context of BRICS, stronger countries are often characterized by aggressive behavior in cyberspace, which can lead to the loss of digital sovereignty by less developed countries.[13]

The key problem is that the contrary viewpoints are not supported by specific data. We are of the opinion that in order to determine the potential for cybersecurity cooperation between the BRICS member countries, it is necessary to:

- Analyze the problems of introducing ICT in each of the countries.
- Carry out a comparative analysis of national cybersecurity strategies.
- Highlight promising areas for cooperation.

Studying these data will allow us to determine the possible level of cooperation and assess the prospects for the formation of a joint strategy.

The BRICS member countries can continue to strengthen their positions in the global economy through the formation of a single digital market. Digital transformation requires an integrated approach. New technologies should not be introduced without control. States should guide the use of technologies and respond flexibly to ongoing

[9] Hans de Bruijn & Marijn Janssen, *Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies*, 34(1) Gov't Info. Q. 1 (2017).

[10] Evgenii Nikitin & Mensah C. Marius, *Unified Digital Law Enforcement Environment – Necessity and Prospects for Creation in the "BRICS Countries"*, 7(2) BRICS L.J. 66 (2020).

[11] Ali Burak & Daricili Barış, *Analysis of the Cyber Security Strategies of People's Republic of China*, 14(28) Güvenlik Stratejileri Dergisi (J. Security Strategies) 1 (2018).

[12] Rodrigo Fracalossi de Moraes, *Whither Security Cooperation in the BRICS? Between the Protection of Norms and Domestic Politics Dynamics*, Global Policy (June 2020) (Feb. 2, 2023), available at https://ssrn.com/abstract=3632389.

[13] Brett Van Niekerk, *South Africa and the Cyber Security Dilemma*, 18(2) J. Info. Warfare 96 (2019).

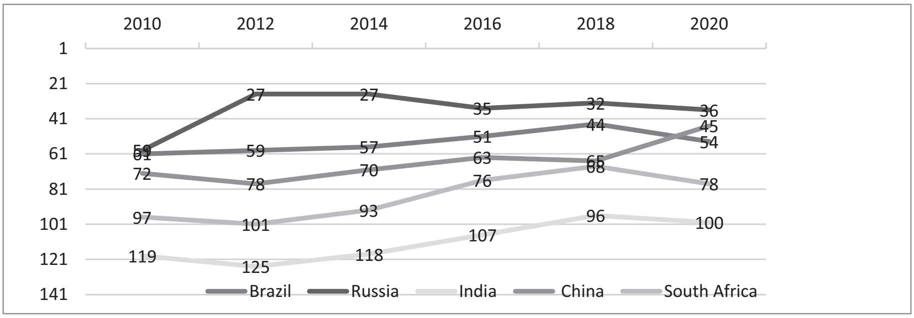
changes. It is impossible to ensure the national cybersecurity of each country without international cooperation. Successful models from other countries should serve as a point of growth to upgrade national cybersecurity strategies.[14] The adoption of a joint cybersecurity strategy among BRICS member countries could significantly increase the influence of this bloc in the international community.

1. E-Government as a Basis for the Formation of a National Cybersecurity System

An integrated approach must be used to assure national cybersecurity. States should guide the use of technologies and respond flexibly to ongoing challenges. The development of e-government and online provision of public services reflects the level of integration of public management of economic digitalization and serves as the basis for the formation of a national cybersecurity system. Only a developed e-government can ensure adequate interaction of cybersecurity subjects at all levels in order to prevent and suppress cyberattacks.[15]

Analysis of the data from the United Nations E-Government Development Index showed that the BRICS member countries are making efforts to introduce ICT. Having examined the data from 2010 to 2020, we see that the indicators of the e-development level do not have positive dynamics in all the countries. This indicates existing problems to be studied in detail (Figure 1).[16]

Figure 1: **E-Government Development Index of the BRICS member countries**



Source: Author, based on UN open data

[14] ITU, *ITU National Cybersecurity Strategy Guide*, International Telecommunication Union (September 2011) (Feb. 2, 2023), available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf.

[15] FCC, *Cyber Security Planning Guide*, Federal Communications Commission (October 2012) (Feb. 2, 2023), available at https://transition.fcc.gov/cyber/cyberplanner.pdf.

[16] Brig V. Anand, *A Perspective on BRICS Development Strategies: Prospects and Issue*, Vivekananda International Foundation, 11 September 2017 (Feb. 2, 2023), available at https://www.vifindia.org/article/2017/september/11/a-perspective-on-brics-development-strategies-prospects-and-issues.

Let us consider the effectiveness of the development of e-government in each of the BRICS member countries. The main aspects for our analysis are the condition of online services, telecommunication technologies and human capital.

1.1. E-Government in the Russian Federation

Russia is the leader in digitalization among the BRICS member states and is ranked 36th on the 2020 United Nations E-Government Survey. Public policy in Russia has consistently emphasized digitalization; however, further development is hampered by the insufficiently high level of information and communication infrastructure, which is rated at 0.7723 in the same UN Survey.[17] This gap is explained by the large size of the country's territory and the harsh climatic conditions in thirty percent of the regions.

Solutions to bridge this gap are included in the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030.[18] Its objectives include the development of the information and communication infrastructure and the creation of a new technological basis for the development of the economy and social sphere. The main priority of the Strategy is to improve the living standards of the population through the widespread use of national ICT.

The Digital Economy national project is being implemented from 2018 to 2024 to achieve the objectives of the Strategy. Its task is to create a stable and secure information and telecommunications infrastructure that allows for the high-speed transmission, processing and storage of large amounts of data available to all organizations and households.[19] Officials plan to develop and launch the Federal Spatial Data Web Portal – a state information system; connect public and local self-government authorities to the Internet; introduce interdepartmental electronic document management using electronic signatures in the activities of federal and regional executive authorities; create a platform to exchange information between the state, citizens as well as profit and non-profit organizations (Digital Profile infrastructure); develop and launch a protected digital environment for audiovisual interaction between governmental authorities, organizations and citizens at the federal, regional, and municipal levels; and launch an Electronic Passport for RF citizens.[20]

[17] 2020 United Nations E-Government Survey (July 2020) (Feb. 2, 2023), available at https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf.

[18] Decree of the President of the Russian Federation, 9 May 2017 (Feb. 2, 2023), available at http://www.kremlin.ru/acts/bank/41919.

[19] 'Digital Economy' National Project, 18 September 2020 (Feb. 2, 2023), available at http://static.government.ru/media/files/3b1AsVA1v3VziZip5VzAY8RTcLEbdCct.pdf.

[20] Digital Public Administration Factsheet, 20 September 2020 (Feb. 2, 2023), available at https://joinup.ec.europa.eu/sites/default/files/inline-.files/Digital_Public_Administration_Factsheets_Sweden_vFINAL.pdf.

1.2. E-Government in China

China is ranked 45th in the 2020 UN Rating. From 2010 to 2018, the country smoothly climbed from 93rd to 68th place. However, in 2020, China made a sharp leap, rising twenty positions at once. At the same time, China came close to the ideal model in terms of the quality of its online services. The index for this indicator was 0.9059.[21]

The active introduction of e-government and the digitalization of government control are driven by economic needs. The largest transnational companies have begun to actively enter the Chinese market. However, investments can only be attracted with the availability of digital tools for prompt cooperation with regulatory agencies and the compliance of the e-government development level with global standards.

The barrier to attracting international capital was the excessive bureaucratization of China's government control system. Each day, government agencies issue a large number of regulations, which are constantly updated and amended. Furthermore, the Golden Bridge Project was launched to ensure their timely distribution. This project aims to create a fundamental infrastructure for national information systems and provide assistance to administrative authorities. The creation of government websites allows individuals and organizations to gain prompt access via the Internet to relevant information and services online.

The development of e-government in China has ensured annual market growth rates of 12% to 17% (10 years before 2017) and opened up the market with a total value of 272.2 billion yuan (about 38 billion dollars).[22]

In May 2019, a national public services platform was launched, which is linked to 46 departments of the State Council and 32 local self-government authorities. This platform improved the general capabilities of the government services on the Internet. As of December 2019, the platform had 339 million registered users, which means that one out of three Internet users in China signed up on the platform.[23] The capabilities of the online service have improved. Administrative approval procedures have been simplified. Many permits can be granted online. Herewith, the number of citizens using e-government services is only 23.4% of the population, which is caused by the digital divide between different segments of the population. There is inequality both in the provision of access to ICT and in its use.

However, China is still considered an emerging economy with tight government control. The state not only encourages the development of ICT but also directs its

[21] Masoud Shayganmehr & Gholam A. Montazer, *A Novel Model for Assessing E-Government Websites Using Hybrid Fuzzy Decision-Making Methods*, 1468 Int'l J. Computational Intelligence Systems (2021) (Feb. 2, 2023), available at https://www.atlantis-press.com/journals/ijcis/125956171/view.

[22] Lin Rubi, *China's E-Government Drive Creates $38bn Market*, Nikkei Asia, 8 October 2019 (Feb. 2, 2023), available at https://asia.nikkei.com/Business/Business-trends/China-s-e-government-drive-creates-38bn-market.

[23] Ji Jing, *China Has Made Remarkable Progress in Delivering E-Government Services*, Beijing Review, 20 July 2020 (Feb. 2, 2023), available at http://www.bjreview.com/Nation/202007/t20200720_800214813.html.

efforts towards establishing state control over the Internet space on its territory, which keeps the rest of the world from not knowing what is going on in China, as we have seen during the COVID-19 pandemic situation.

> The "Great Firewall" prevents Internet users in China from visiting many foreign websites for one reason or the other and blocking them completely.[24]

Internet access capabilities differ significantly among the different departments in China. Metropolitan areas and large cities have a developed network and robust websites for local government authorities. Thus, the 2020 UN rating cites the unified system of public services in Shanghai as an example of successful e-government.[25] Over 29.21 million individuals and over 2.08 million legal entities are registered on the municipal e-government portal. The portal not only allows users to handle a wide range of routine matters, such as registering a business and paying utility bills, but also provides information on the various types of emergencies and the emergency services that are available to deal with them.

The level of access to information and communications technologies in Shenzhen, Hangzhou and Guangzhou in Eastern China is nearly three times the national average.[26] However, in Longnan in the Gansu province, Bijie and Tongren in the Guizhou province, Ganji in the Sichuan province and Hetian in the Xinjiang province, network access is only half the national average.[27]

Another reason for the gap is the large proportion of elderly people (18.1% of the total[28]). Furthermore, 17.95% of the population is below the age of fifteen years, and as a result, they are unable to use digital services due to age limitations.[29]

[24] Sonali Chandel et al., *The Golden Shield Project of China*: *A Decade Later an In-depth Study of the Great Firewall*, in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 111 (2019).

[25] Jing, *supra* note 23.

[26] Chuanglin Fang et al., *The Sustainable Development of Innovative Cities in China: Comprehensive Assessment and Future Configuration*, 24 J. Geographical Sci. (2014) (Feb. 2, 2023), available at https://www.researchgate.net/publication/267340319_The_sustainable_development_of_innovative_cities_in_China_Comprehensive_assessment_and_future_configuration.

[27] Zhouying Song et al., *China's Prefectural Digital Divide: Spatial Analysis and Multivariate Determinants of ICT Diffusion*, 52 Int'l J. Info. Mgmt. (Article 102072) (2020).

[28] Huang Lanlan et al., *Narrowing 'Digital Divide': China Steps up Efforts to Better Serve the Elderly in Digital Age*, Global Times, 2 December 2020 (Feb. 2, 2023), available at https://www.globaltimes.cn/content/1208770.shtml.

[29] C. Textor, *Population Distribution in China in 2020, by Broad Age Group*, Statista, 19 May 2021 (Feb. 2, 2023), available at https://www.statista.com/statistics/251524/population-distribution-by-age-group-in-china/.

1.3. E-Government in Brazil

Over the past two years, Brazil has moved down in the UN rating significantly (from 44th to 54th). However, the quality and level of the online services provided are very high. A peculiar feature of Brazil is the constant feedback between government service providers and consumers. One of the distinguishing features of Brazil that makes it stand apart from the other BRICS countries is the way in which its citizens actively contribute to the creation of new digital projects and in the improvement of those that already exist. The resolution of digital issues at a consumer level is a unique practice that has the potential to be of long-term benefit in any country's digital policy.[30]

The National Debureaucratization Council coordinates the Effective Brazil (Brasil Eficiente) program, which aggregates the measures of all federal public service institutions, including ministries and the presidency. The goal of the program is to modernize relations between the government and society and make life easier for citizens and organizations that use public services. The program aims to optimize public services, simplify the procedure for obtaining services, and reduce costs.[31] For example, Decree No. 9094, dated 17 July 2017, states that federal government authorities should not request documents or information from citizens who are already registered in federal government databases.

The first version of the Brazilian Digital Government Strategy was implemented in 2016–2018. Several digital identity projects have been recently completed, for example, Brazilian driver's licenses, Brazilian voting IDs (Título Eleitoral), worker's IDs (Carteira de Trabalho) and the electronic version of the National ID Card and Registry (enacted by Law no. 13,444/2017). The delivery of digital services has also been largely improved with the implementation of a services portal that aggregates information (or e-services) from the majority (or all) of Brazilian federal entities.[32]

In May 2018, an updated version of the Strategy was presented. The document sets five strategic goals: (a) promoting the availability of open government data; (b) promoting transparency through ICTs; (c) expanding and innovating in the provision of digital services; (d) exchange and integration of data, processes, systems, services and infrastructure and (e) improving social participation in the life cycle of public policies and services.[33]

[30] UNCTAD, *Digital Economy Report 2019*, United Nations, 4 September 2019 (Feb. 2, 2023), available at https://unctad.org/system/files/official-document/der2019_en.pdf.

[31] The Effective Brazil Program, Brazilian Government Portal, 16 December 2017 (Feb. 2, 2023), available at http://www.brasileficiente.gov.br/.

[32] Digital Government Review of Brazil, *Towards the Digital Transformation of the Public Sector*, OECD Digital Government Studies, 28 November 2018 (Feb. 2, 2023), available at https://doi.org/10.1787/9789264307636-en.

[33] Brazilian Digital Government Strategy, 21 May 2018 (Feb. 2, 2023), available at https://www.governodigital.gov.br/EGD.

An important result of the Strategy was the creation of the National Digital Transformation System and the Interdepartmental Committee for Digital Transformation (CIT Digital), which became the main controlling bodies in the implementation of the digital policy.[34]

1.4. E-Government in South Africa

The Republic of South Africa (RSA) also dropped in the UN rating, moving from 68th to 78th place. At the same time, the provision of public online services and the digital literacy of the population are both at decent levels, with an index of 0.7471 and 0.7371, respectively. However, the telecommunications infrastructure index is low at 0.5832. The main reason for the slowed development is the insufficient coverage of the country's territory with fixed (wired) broadband lines, with only 1.92 per 100 people connected to the Internet.[35]

We should take note of the objective reasons impeding the development of ICT in South Africa. The main reason is the geographical remoteness of the African continent, which entails high costs for the construction and operation of the necessary digital infrastructure.

For this reason, the development of ICT in the RSA is centered in densely populated districts and metropolitan areas. The provided services are shaped according to the Western model and focused on the needs of the educated city dweller. A large-scale survey of government online services was conducted by research scholars, Shawren Singh and Bob Travica. They found that all government websites in South Africa, which is a country with eleven official languages, only provide information in English.[36]

The development level of e-government in the RSA can only increase if Western models are adapted to the peculiar features of the local population. Furthermore, the technological complexity and high cost of projects for the development of information and communication infrastructure in Africa predetermine the need to attract investments and specialists from more developed countries. This area holds a lot of potential for the development of cooperation among the BRICS countries.

1.5. E-Government in India

India is significantly behind other BRICS member countries in terms of its position in the UN rating, occupying the 100th place at present. However, a contradictory

[34] OECD, *Policies for Digital Transformation: Recommendations for a Whole-of-Government Approach*, OECD iLibrary, 11 March 2019 (Feb. 2, 2023), available at https://www.oecd-ilibrary.org/sites/95ac155a-en/index.html?itemId=/content/component/95ac155a-en.

[35] UN Study E-Government 2020 (Feb. 2, 2023), available at https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf.

[36] Tendani Mawela et al., *E-Government Implementation: A Reflection on South African Municipalities*, 29(1) South African Computer J. 147 (2017).

picture comes up when analyzing individual indicators. The level of providing online government service in India is 0.8529. According to this indicator, India is inferior only to China and Brazil among the BRICS member countries. The high quality of providing public services is ensured by the government's constant efforts to implement digital initiatives.[37]

The Digital India Program was launched in 2014 to ensure a high quality of public services. The goal of this program is to transform India into a digital society and a knowledge economy. The program is implemented in three main areas: the creation of a digital infrastructure useful for citizens, e-government and on-demand services and digital empowerment of citizens.[38]

However, the majority of citizens do not have access to the highly efficient government services available online. According to projections made by the UN for its 2020 rating, India's information and communication infrastructure development index was estimated to be 0.3515 and the level of the population's computer literacy was estimated at 0.5848. The 2017–2018 National Sample Survey showed that only 23.8% of Indian households had Internet access. In rural households (66% of the population), access to the Internet is at 14.9%, whereas in urban households access is at 42%[39] The measures taken by the Indian government to establish control over the Internet space also reduce the availability of e-government services. In this particular scenario, the issue that arises is not simply the restriction of the consumable content but rather the complete prohibition of access to the global network. In 2019, there were 121 Internet outages in India. For instance, in August 2019, the government in the states of Jammu and Kashmir completely blocked Internet access for 175 days to prevent riots,[40] and therefore it was impossible to receive e-government services, especially at a time of riots and other internal disturbances. India's multiculturalism is another problem. E-government websites mainly post information in English. Even though the majority of the population does speak English, in a country with twenty-two officially constitutionally recognized languages, finding content in the local language is a challenge.[41]

[37] PIB Delhi, *High Performance Computing (HPC) and Information Communication Technologies (ICT) discussed at BRICS Working Group Meeting*, Ministry of Science and Technology, 30 May 2021 (Feb. 2, 2023), available at https://www.pib.gov.in/PressReleasePage.aspx?PRID=1722819.

[38] Vision of Digital India, 18 November 2014 (Feb. 2, 2023), available at https://digitalindia.gov.in/content/vision-and-vision-areas.

[39] Digital Daan, Digital Empowerment Foundation (Feb. 2, 2023), available at https://www.digitaldaan.in/.

[40] Berhan Taye, *Internet Shutdowns in 2019: A Global Overview*, Access Now, 22 February 2019 (Feb. 2, 2023), available at https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf.

[41] UN, *E-Government Development Index*, Digital Russia, 28 August 2018 (Feb. 2, 2023), available at https://d-russia.ru/wp-content/uploads/2018/08/E-Government-Survey-2018_FINAL-for-web.pdf.

Nevertheless, India is actively trying to eliminate the digital divide. The country has the largest national identification system, Aadhaar, with biometric and demographic data of over a billion users. The poorest segments of the population, who had never previously possessed an identity card, were digitally identified through this system. As a result of this system, they are able to gain access to social benefits and Internet banking. There are over 1 billion bank accounts and mobile telephones connected to Aadhaar, and the database has recorded over $12 billion in financial transactions.[42]

Government initiatives within the framework of the Digital India Program focus on connecting rural communities to the network; lowering prices of Internet-connected phones and data transfer calling plans; promoting e-wallets and creating free Wi-Fi hotspots among others endeavors.[43]

2. Strategic Cybersecurity Activities

The most authoritative measurement of a state's cybersecurity level is the Global Cybersecurity Index, which is calculated by the International Telecommunication Union (ITU). The study compares the achievements of the participating countries in these areas.

According to the Global Cybersecurity Index (2018), only Russia and China have a high level of cybersecurity among the BRICS member countries; the remaining three countries have an average level. The countries of the bloc have a significant spread in the ratings, occupying from 26th to 70th places out of 194 (Table 1).

Table 1: **The Global Cybersecurity Index 2018 of the BRICS member countries**

Country	Level	Rating
Russia	high	26
China	high	27
India	high	47
South Africa	medium	56
Brazil	medium	70

Source: Author based on ITU open data (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)

[42] Noor A. Samion & Azlinah Mohamed, *Innovation of National Digital Identity: A Review*, 9(1.2 Special Issue) Int'l J. Advanced Trends in Computer Sci. and Engineering 151 (2020).

[43] Sharada P. Mohanty et al., *On the Design of a Youth-Led, Issue-Based*, *Crowdsourced Global Monitoring Framework for the SDGs*, 11(23) Sustainability (Article 68399) (2019).

The foundation for ensuring cybersecurity at the national level is a program document determining the state's policy in this area. Currently, all BRICS member countries have adopted such a document. However, we can see significant differences in the terminology and main directions of implementation (Table 2).

Table 2: **Cybersecurity strategies of the BRICS member countries**

Country	Year	Document title
Russia	2010 (2016)	Information Security Doctrine of the Russian Federation
India	2013	National Cybersecurity Policy
South Africa	2015	The National Cybersecurity Policy Framework
China	2017	Cybersecurity Law of the People's Republic of China
Brazil	2020	Brazilian National Cybersecurity Strategy E-Cyber

Source: Author, based on open data

Let us compare the goals and objectives of the national strategies of the BRICS member countries, the response procedure to cyberattacks and measures to counter cybercrimes. Russia uses the term "information security" instead of the concept of cybersecurity. Information security involves protecting information networks and maintaining the sovereignty, territorial integrity, defense, and security of the state.

In terms of cybersecurity, Russia is significantly ahead of other EAEU member states. It ranks 26th in the rating and belongs to the group of countries with a high level of cybersecurity. Its readiness to repel cyberattacks is 86.3%.[44]

The Doctrine of Information Security of the Russian Federation was first adopted in 2000. The updated document has been in effect since 2016. The subject of regulation is not only the security of the hardware and software complex but also the content of information transmitted using the global network.

Criminal liability for computer information crimes has been stipulated in the Russian legislation since 1996. Law enforcement practices are constantly monitored and criminal justice standards governing liability for crimes involving information and communication technologies are being improved. In the first quarter of 2021, criminal liability for libelous actions committed using information and telecommunication networks was introduced, and criminal liability for incitement to narcotics committed through telecommunication networks was toughened.

[44] ITU, *Global Cybersecurity Index (GCI)*, ITU Publications (2018) (Feb. 2, 2023), available at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

International cooperation in the field of information security is determined by a separate regulatory instrument – the Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security until 2020.[45]

China is also committed to the decisive role of the state in ensuring cybersecurity. The main regulatory document is the Cybersecurity Law of the People's Republic of China, which entered into force on 1 June 2017. The law aims to ensure cybersecurity; protect the sovereignty and national security of cyberspace and social and public interests; protect the legal rights and interests of citizens, legal entities and other organizations; and contribute to the healthy development of informatization of the economy and society.[46]

According to the law, the state undertakes to contribute to widespread Internet access, increase the level of network services, and guarantee the legal, well-ordered and free distribution of network information.

Network users are responsible for upholding the Constitution and laws, keeping the peace and respecting public morality. A multi-layered cybersecurity protection system has been established according to this law:

1. Developed and implemented national standards for network products and services. These standards include the Basic Level of Information Security Technologies for Classified Cybersecurity Protection (GB/T 22239–2019), Guidelines for Classified Cybersecurity Protection (GB/T 25058–2019) and Guidelines for the Classification of Classified Cybersecurity Protection (GB/T 22240–2020).[47]

2. The Cybersecurity Verification Measures were adopted and are to be implemented by network operators. These measures should prevent unauthorized access to the Internet and ensure user identification and preliminary verification of posted content. If the information poses a threat to the national security of the state, the operator should block it and report it to the appropriate public authorities.[48] Additionally, the posted content is constantly monitored by network operators and authorized state bodies to exclude state security and public moral risks.[49]

3. Outlined requirements for the protection of the critical information infrastructure. The main ones include storage of information on the territory of mainland

[45] Information Security Doctrine of the Russian Federation, 29 December 2008 (Feb. 2, 2023), available at https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf.

[46] Cybersecurity Law of the People's Republic of China, 29 June 2018 (Feb. 2, 2023), available at https://www.chinafile.com/ngo/laws-regulations/cybersecurity-law-of-peoples-republic-of-china.

[47] Susan Xuanfeng Ning & Han Wu, *China: Cybersecurity Laws and Regulations*, ICLG, 2 November 2020 (Feb. 2, 2023), available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/china.

[48] NCES, Security Management, National Center for Education Statistics, 2 November 2020 (Feb. 2, 2023), available at https://nces.ed.gov/pubs98/safetech/chapter4.asp.

[49] Cybersecurity Verification Measures, 20 April 2020 (Feb. 2, 2023), available at http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm.

China, annual inspections of the condition of networks by service providers and selective testing of networks by government agencies.

China also adopted the International Strategy of Cooperation on Cyberspace on 1 March 2017. It emphasizes the need for international cooperation to ensure cybersecurity. In addition to the development of a global Internet governance system, it proposes creating a system of international behavioral rules and norms for states regarding cyberspace. It takes note of China's aspiration to participate in bilateral and multilateral agreements in this field and promote practical cybersecurity cooperation among the BRICS members.[50]

India adopted their National Cyber Security Policy in 2013. The document is a framework and defines a development strategy in this area. The main goals are as follows:

1. To create a safe cyber ecosystem in the country, form adequate trust and confidence in IT systems and transactions in cyberspace, and thereby enable the wider implementation of IT in all sectors of the economy.

2. To develop effective partnership relations between the public and private sectors based on joint participation in cyberspace security assurance.

3. To create a cybersecurity and privacy culture that provides for the users' responsible behavior and actions through effective communication and promotion strategies.

The large number of cyberattacks coming from other states as well as the discovery of vulnerabilities in the existing system led to adjustments to the digital policy. The development of a new National Cybersecurity Strategy for 2020–2025 was announced at the end of 2019.[51] However, it has not been published yet. The steps that have already been taken show that there is an emphasis on ensuring digital sovereignty and strengthening state control over cyberspace. In accordance with the Law on Personal Data of 2019, their storage is localized on the territory of India. Furthermore, the Defense Cyber Agency of India's tripartite Armed Forces Command was formed, whose task is to counter cyberthreats.[52]

Nevertheless, public-private partnerships continue to play a significant role in cybersecurity. The Indian modern digital policy implements the principle of joint but differentiated responsibility with a gradual increase in the role of the state in cybersecurity assurance.[53]

[50] Tian Shaohul, *International Strategy of Cooperation on Cyberspace*, News.cn, 1 March 2017 (Feb. 2, 2023), available at http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_3.htm.

[51] David Chinn et al., *Perspectives on Transforming Cybersecurity*, McKinsey & Company (March 2019) (Feb. 2, 2023), available at https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx.

[52] *India to Have Defence Cyber Agency in May; Rear Admiral Mohit to Be its First Chief*, India Today: News, 30 April 2019 (Feb. 2, 2023), available at https://www.indiatoday.in/india/story/india-defence-cyber-agency-may-rear-admiral-mohit-1513381-2019-04-30.

[53] *India's Trillion-Dollar Digital Opportunity*, Ministry of Electronics and Information Technology, 28 April 2019 (Feb. 2, 2023), available at https://www.digitalindia.gov.in/ebook/MeitY_TrillionDollarDigitalEconomy.pdf.

The Republic of South Africa adopted the National Cybersecurity Policy Framework (NCPF) on 4 December 2015. The goals include:

1. To promote a cybersecurity culture and to require compliance with the minimum security standards.

2. To strengthen the acquisition of intelligence information as well as investigations, prosecutions and lawsuits related to the prevention and suppression of cybercrimes, cyberwars, cyberterrorism and other malicious cyber acts.

3. To establish partnerships between the state, private and public sectors for the purpose of implementation of national and international action plans.

4. To ensure the protection of the National Critical Information Infrastructure (NCII).

5. To improve the legal framework that regulates cyberspace.

6. To maximize human potential.

A peculiar feature of the NCPF is its emphasis on the participation of the private sector, government, academic world and the general public in ensuring cybersecurity.

The lack of legal regulation in the field of cybersecurity in South Africa is a serious issue. However, since the adoption of the NCPF, significant progress has been made: the Critical Infrastructure Protection Act was passed and a draft Law on Cybercrimes and Cybersecurity was elaborated. The latter defines the concept of cybercrimes and introduces criminal liability for Internet crimes.[54]

Another problem is the lack of cybersecurity skills. To solve this problem, the Department of Communications and Postal Services established a Cybersecurity Center, which organizes civic education in this field with the participation of the public and private sectors.[55]

South Africa considers national cybersecurity a multifaceted concept implemented with the participation of many interested parties. The main efforts are focused on training and generating human potential, civic education and awareness, research and development of systems and cybercrime control.[56]

Brazil began shaping its legal cybersecurity framework in 2018 with the adoption of the National Information Security Policy.[57] The National Cybersecurity Strategy (E-Cyber) was adopted on 5 February 2020. It became the first module in the legal support of information security and defines the following strategic goals:

[54] Cybersecurity Bill, 12 July 2017 (Feb. 2, 2023), available at https://pmg.org.za/bill/684/.

[55] *Deputy Minister Pinky Kekana: CEO Forum for Cybersecurity*, South African Government, 26 March 2019 (Feb. 2, 2023), available at https://www.gov.za/speeches/deputy-minister-pinky-kekana-ceo-forum-cybersecurity-26-mar-2019-0000.

[56] Noluxolo Kortjan, *A Cyber Security Awareness and Education Framework for South Africa* (November 2013) (Feb. 2, 2023), available at https://core.ac.uk/download/pdf/145053774.pdf.

[57] Decree of the President of the Republic of Brazil, 28 December 2018 (Feb. 2, 2023), available at http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm.

- to make Brazil more prosperous and secure in the digital environment;
- to increase Brazil's resilience to cyberthreats;
- to increase the cybersecurity effectiveness of Brazil in the international arena.

The Strategy was based on the principle of organizing joint activities of the public sector, the private sector, the academic world and society. There are eight types of Computer System Information Response Teams (CSIRTs) outlined to counter cyberattacks:

- National Responsibility Center;
- International Coordination Centers;
- CSIRT for critical infrastructures (energy, finance, telecom);
- CSIRT of providers;
- Corporate CSIRT;
- Academic CSIRT;
- CSIRT of the state authority;
- Military CSIRT.

The main responsibility to protect the critical infrastructure is assigned to companies operating in this area. They should create cybersecurity management structures that include the establishment of guidelines, manuals, classifications and procedures for handling incidents, as well as security rules applicable to all employees, contractors and suppliers.[58]

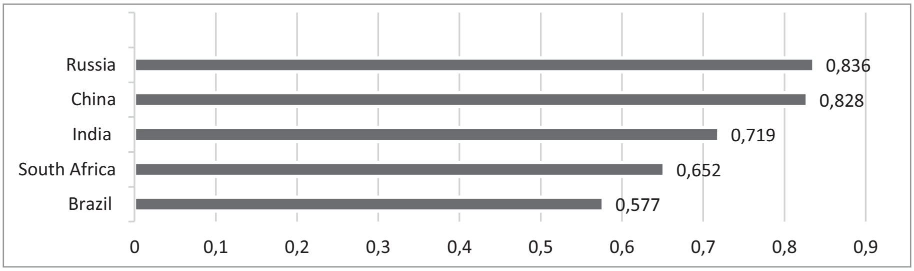
In general, E-Cyber is rather declarative; it defines the main lines of cybersecurity assurance but does not provide for specific measures for their implementation.

All of the BRICS member countries make targeted efforts to implement the key lines of cybersecurity. However, their national strategies set different priorities. Russia and China consider cybersecurity to be one of the components of state sovereignty, imposing strict state control over its provision. India, Brazil and South Africa, on the contrary, are making efforts to increase global information exchange and organize public-private partnerships in cybersecurity.

This difference in the approaches hinders closer interaction. However, an analysis of the results of the Global Cybersecurity Index (2018) shows that the countries with state control governing cyberspace have a higher cyber protection level. While Russia is ready to repel cyberattacks and counter cybercrimes by 83.8%, this indicator in Brazil is only 57.7% (Fig. 3).

[58] Decree of the President of the Republic of Brazil No. 10.222 'On Approval of the National Cybersecurity Strategy,' 5 February 2020 (Feb. 2, 2023), available at https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419.

Figure 3: **The level of cybersecurity of the BRICS member countries**



Source: Author, based on ITU open data (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)

We believe that the digitalization of the economy and public administration, which has grown significantly during the pandemic, has increased the dependence of the states on the condition of cybersecurity. Repeated cyberattacks have the potential to seriously damage national economies. The existence of different cyberattack regulatory models in the private sector complicates the formulation and implementation of universally acceptable rules and standards necessary to ensure cyber defense. This predetermines the need for a state-oriented approach to effective containment in cyberspace and provides grounds for a further rapprochement of the BRICS member countries.

3. Cybersecurity Cooperation of the BRICS Member Countries

The joint strategic goal of the BRICS member countries to strengthen cybersecurity cooperation was officially formulated in 2013. The eThekwini Declaration which was signed in Durban, South Africa on 27 March 2013 states:

> We believe it's important to contribute to and participate in a peaceful, secure, and open cyberspace and we emphasize that security in the use of information and communication technologies through universally accepted norms, standards and practices is of paramount importance.[59]

The areas of cooperation were specified at a meeting of the National Security Advisors held at the same summit: first, preventing cyberspace from turning

[59] *eThekwini Declaration v. BRICS Summit*, Durban, South Africa, 27 March 2013 (Feb. 2, 2023), available at http://www.nkibrics.ru/system/asset_docs/data/53da/485c/676c/761f/8d73/0000/original/V_BRICS_SUMMIT_-_ETHEKWINI_DECLARATON_MARCH_27__2013_DURBAN__SOUTH_AFRICA.docx?1406814300.

into a platform for recruiting terrorists and spreading radical ideologies; second, punishing not just the attackers, but also the organizers of cyber terrorism and cybercrimes and third, developing international cooperation through multilateral mechanisms within the UN framework. The joint strategic goal of reforming global cyberspace governance laid a solid strategic foundation for BRICS cybersecurity cooperation. The major challenges these countries face require further development of their agenda in order to help developing countries gain greater authority in the governance system.[60]

However, cooperation has been limited to the coordination of special positions. The 2020 Summit did not result in the adoption of a program document on the cybersecurity interaction of the BRICS member countries. The member countries proposed that they continue working on concluding an appropriate five-way agreement.[61] This is because the differences in the types of regimes lead to the appearance of mistrust between the countries and the imbalance of power inside the bloc raises concerns in the form of potential unequal agreements.[62]

During the period of cooperation within the BRICS framework, Russia entered into bilateral agreements on information security with all of the member countries.

The Agreement between the Government of the Russian Federation and the Government of the Federal Republic of Brazil on cooperation in the field of international information and communication security, signed on 14 May 2010 in Moscow, was the first document of its kind.

The main areas of cooperation enshrined in this document do not contain specific bilateral measures but serve as frameworks and declarations. They contain the following items:

1. Determination, approval and implementation of the necessary joint measures required to ensure international information and communication security.

2. Creation of a joint structure for the prevention, detection, elimination and response to information security threats.

3. Examination, research and assessments in the field of information and communication security, including cooperation between the parties in the areas of technology and science.

4. Development of interaction within the framework of Internet governance forums on information and communication security issues.

[60] Gao Wanglai, *BRICS Cybersecurity Cooperation: Achievements and Deepening Paths China International Studies*, PressReader.com, 20 January 2018 (Feb. 2, 2023), available at https://www.pressreader.com/china/china-international-studies-english/20180120/281513636564569.

[61] *BRICS National Security Advisors discuss topical issues of security cooperation*, Official website of the Russian BRICS Chairmanship in 2020, 18 September 2020 (Feb. 2, 2023), available at https://eng.brics-russia2020.ru/news/20200918/582132/BRICS-National-Security-Advisors-discuss-topical-issues-of-security-cooperation.html.

[62] Moraes, *supra* note 12.

5. Ensuring the information and communication security of national critically important infrastructures.

6. Development and implementation of an approved policy for the use of electronic digital signatures and information protection during international information exchange.

7. Exchange of information on legislation pertaining to information and communication security issues in the Russian Federation and the legislation of the Federal Republic of Brazil.

8. Development and improvement of the international legal framework as well as the practical mechanisms of cooperation between the parties in strengthening international information and communication security.

9. Cooperation on the international information and communication security problems within the framework of existing international organizations and forums.

10. Knowledge exchange, specialist education and organization of task meetings, conferences, seminars and other forums of the authorized representatives and experts in information and communication security of the parties involved in the agreement.[63]

The agreement notes that the essential principle of cooperation is non-interference in the internal affairs of another state. The agreement is, thus far, only declarative. Bilateral events are not held, but the countries continue to cooperate in this area within BRICS.

On 8 May 2015, the Government of the Russian Federation and the Government of the People's Republic of China signed an agreement on international information security cooperation.[64] Over the five years since the conclusion of the previous bilateral agreement, the digitalization of economic and social life has reached a new level. This led to the globalization of cyberspace and the appearance of new types of information threats.

Between 27 November 2013 to 15 December 2014, hackers stole personal information (phone numbers, email and postal addresses, credit and debit card numbers and PINs) from 110 million customers of Target Corporation, the third largest retail chain in the United States. As a result, American financial institutions suffered losses of over $200 million. In its 2015 Cyber Security Intelligence Index, IBM reported that nearly two-thirds of cyberattacks focused on three industries: finance and insurance, information and communications, and production.[65]

[63] Agreement between the Government of the Russian Federation and the Government of the Federative Republic of Brazil on International Information and Communication Security, 14 May 2010 (Feb. 2, 2023), available at http://docs.cntd.ru/document/902366519.

[64] Agreement between the Government of the Russian Federation and the Government of the People's Republic of China on international information security cooperation, 8 May 2015 (Feb. 2, 2023), available at http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1.

[65] *42 Cyber Attack Statistics by Year: A Look at the Last Decade*, Sectigo Store, 8 December 2016 (Feb. 2, 2023), available at https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/.

During this period, the actions of cybercriminals moved from the national to the international level and affected the activities of not only economic organizations but also state institutions. On 3 June 2013, hackers from the group Anonymous disrupted the websites of the Turkish President, the Prime Minister and several government agencies. Thus, criminals supported anti-government demonstrations in the country.[66]

In response to the new challenges, the agreement formulates relevant types of cyberthreats, such as the use of ICT to interfere in the internal affairs of states; disrupt public order; incite interethnic, interracial and interfaith hostility; promote racist and xenophobic ideas and theories that generate hatred and discrimination; incite violence and instability and destabilize the internal political and socio-economic situation; violate state governance; and cause economic and other damage.[67] The general provisions of this agreement include such terms as computer attack, unlawful use of information resources, and unauthorized interference with information resources.[68]

The main areas of cooperation in this agreement are more clearly elaborated. The number of areas of cooperation has grown from ten to sixteen. The content has become more specific. The agreements reached are implemented with a high degree of precision.

The establishment of cooperation in the scientific and research areas was a promising area of development. The agreement formulates specific measures: promotion of scientific research in international information security; joint research projects; joint training of specialists; and student, graduate student and lecturer exchange programs between specialized higher educational institutions.

By September 2013, thirteen Russian-Chinese educational associations and 124 general educational programs were established.[69] Moreover, the implementation of a joint project of Moscow State University and the Beijing Polytechnic Institute to found the Russian-Chinese University in Shenzhen was a significant achievement. Students at this university are given lectures in three languages, and graduates of the Russian-Chinese University will be able to receive diplomas from both the

[66] Major Hacker Attacks in 2001–2016: Timeline, TASS, 18 December 2016 (Feb. 2, 2023), available at https://tass.ru/info/1408961.

[67] ITU, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, International Telecommunication Union, 23 September 2012 (Feb. 2, 2023), available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf.

[68] UN, *Information and Communication Technology Policy and Legal Issues for Central Asia*, United Nations Economic Commission for Europe, 18 December 2020 (Feb. 2, 2023), available at https://unece.org/DAM/ceci/publications/ict.pdf.

[69] European Commission, *Education and Training Monitor*, European Commission, 14 March 2019 (Feb. 2, 2023), available at https://ec.europa.eu/education/sites/default/files/document-library-docs/volume-1-2019-education-and-training-monitor.pdf.

Russian and the Chinese universities. The number of students that participated in the exchange program exceeded 90 thousand students.[70]

In June 2019, Russian President Vladimir Putin and Chinese President Xi Jinping signed the Joint Statement between the People's Republic of China and the Russian Federation on the Development of the Comprehensive Partnership and Strategic Cooperative Relations Entering a New Era in Moscow. This statement declared 2020–2021 as the Year of Russian-Chinese Scientific, Technical and Innovative Cooperation. The parties reached an agreement on a plan of action to expand the mutually beneficial cooperation between research centers, educational organizations and innovation clusters of the partnering states and to promote the growing effectiveness of joint scientific, technical and research projects. They signed a Road Map of the Russian-Chinese cooperation in the fields of science, technology and innovation for the period 2020–2025, which provides for the realization of over 1,000 joint activities.[71]

Another promising area of development was the deepening of cooperation and coordination of the activities between Russia and China on ensuring international information security within the framework of international organizations and forums. The need to deepen cooperation within the BRICS was noted separately.[72] At the 2015 Ufa Summit, the BRICS leaders decided to create a task force on cooperation in the ICT sphere. In November 2016, the Communications Ministers of the BRICS member countries agreed on a common goal of creating a digital partnership. In January 2017, the China Council for the BRICS Think Tank Cooperation (CCBTC) was established. In May, the CCBTC convened a Cyber Economy and Cybersecurity Symposium attended by relevant experts from the BRICS member countries and presented written proposals for the BRICS Summit in Xiamen to be held in September of that same year.[73]

Also of note, the bloc outlined cooperation between the competent law enforcement authorities of Russia and China to investigate cases related to the use of ICT for terrorist and criminal purposes as well as in the field of computer incident response.[74]

Following the signing of the agreement, both sides acknowledged the need to develop cooperation in this area. However, they did not agree on specific measures,

[70] *The student exchange volume between Russia and China has exceeded 90 thousand people*, RIA Novosti, 16 September 2019 (Feb. 2, 2023), available at https://ria.ru/20190916/1558731168.html.

[71] *Russia and China opened the Years of Scientific, Technical and Innovative Cooperation*, Russian Government, 12 September 2021 (Feb. 2, 2023), available at http://government.ru/news/40273/.

[72] VII BRICS Summit: 2015 Ufa Declaration, 7 September 2015 (Feb. 2, 2023), available at http://www.brics.utoronto.ca/docs/150709-ufa-declaration_en.html.

[73] Wanglai, *supra* note 60.

[74] UNODC, *The Use of Internet for Terrorist Purposes* (2012) (Feb. 2, 2023), available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

likely due to the close relationship between the activities of the competent authorities and the security of the state. The joint use of information on the existing and potential risks and information security threats can lead to the vulnerability of the state's critical infrastructure and damage national cybersecurity.

Notably, the text of the agreement contains provisions designed to minimize the risks of cooperation. The agreement provides that each party has an equal right to protect the information resources of its state from unlawful use and unauthorized interference, including from computer attacks on them, and shall not take similar actions in relation to the other Party.

On 15 October 2016, the Government of the Russian Federation and the Government of the Republic of India signed a cooperation agreement on the use of ICT.[75] The following threats were highlighted for the first time in this agreement:

- The harmful use of ICTs aimed at undermining the sovereignty, violating territorial integrity and threatening international peace, human rights, freedom of expression, security and strategic stability.
- Malicious attacks on the critical information infrastructure, which can undermine the safe and stable functioning of global and national information and communication networks, including actions capable of causing economic damage.
- Dissemination of information through the use of ICTs with the intent to disrupt public order, community and social harmony as well as to undermine government control.

Human rights, community and social harmony are protected priorities. This is consistent with the main directions of the Cybersecurity Strategy of India, which considers enterprises and organizations of the private sector and civil society institutions to be the main subject of security regulations in this area. The Indian Information Technology Act aims to prevent all forms of hacking, hijacking and hacktivism.

As a result, one of the highlighted areas of cooperation is an increase in transparency, accountability and inclusiveness in the management of the global Internet network and maintaining its security and stable operation.

On 15–16 February 2018, security advisers held bilateral consultations to realize the agreement. The parties emphasized the need to prevent the use of cyber technologies for criminal and terrorist purposes, also pointing out the need to develop rules for the behavior of the states in this area with the UN in a coordinating role. The parties confirmed their intention to expand practical cooperation on security issues in the use of ICTs, including exchanging data on new challenges in this area and information containing technical and confidential data and capacity building, including through the exchange of ICTs to counter their use for criminal

[75] Agreement between the Government of the Russian Federation and the Government of the Republic of India on cooperation in the field of security in the use of information and communication technologies, 15 October 2016 (Feb. 2, 2023), available at http://docs.cntd.ru/document/420384231.

and terrorist purposes.[76] However, the insufficient consistency of the positions led to a lack of specific results. Despite this, the countries continue to hold political dialogues on cybersecurity to further expand cooperation.

On 4 September 2017, the Government of the Russian Federation and the Government of the Republic of South Africa signed an agreement on international information security cooperation.[77] The language used to describe cyber threats and areas of cooperation is similar to the agreements with other BRICS member countries. The insufficient level of infrastructure development and provision of access to ICT in South Africa made cooperation in cybersecurity research and joint research projects a top priority. Cooperation in this area is realized in a public-private partnership.

In January 2018, representatives of the business community of South Africa visited RTI JSC to implement the Safe City project. The project involves the establishment of municipal centers for monitoring and managing the urban environment as well as upgrading the relevant infrastructure in South Africa. System integration solutions and technologies developed by a Russian company will serve as the project's software foundation.

In October 2020, the largest research project on the development of digital infrastructure in South Africa was launched. Researchers from the BRICS member countries will carry out joint research to develop an intercontinental quantum communication channel. The channel will be 10,000 kilometres long and will connect the universities participating in the project in South Africa and China. Russian specialists are developing new optical fiber technologies; China will provide quantum satellite communications; India will model fiber-optic communications and South Africa will be the lead executor of the project.[78]

This study will lay the foundation for the development of IT communications in all member countries since quantum communications provide an unprecedented level of information security. We firmly believe that the fact that Russia has bilateral cybersecurity agreements with all of the BRICS member countries is an essential achievement that can serve as a launching pad for entering into multilateral agreements.

[76] *Russia and India agreed to expand cybersecurity cooperation*, RIA Novosti, 16 February 2018 (Feb. 2, 2023), available at https://ria.ru/20180216/1514801963.html.

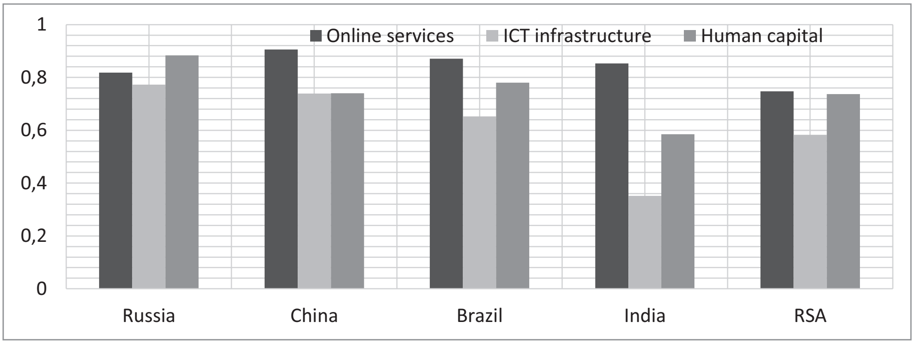
[77] Agreement between the Government of the Russian Federation and the Government of the Republic of South Africa on international information security cooperation, Garant, 4 September 2017 (Feb. 2, 2023), available at https://base.garant.ru/71764786/.

[78] STI overview: Five-Year Anniversary of Cooperation in Science, Technology and Innovation under the Memorandum of Understanding, BRICS, 14 March 2020 (Feb. 2, 2023), available at https://brics-russia2020.ru/images/113/91/1139196.pdf.

Conclusion

Thus, despite significant differences in the development of e-government, each of the BRICS member countries has high achievements in one or several indicators (Fig. 2).

Figure 2: **The standing of the BRICS member countries as measured by the main indicators of the E-Government Index**



Source: UN Study E-Government 2020

The most significant progress has been made in the provision of digital public services, ranked at 0.74–0.90. All countries have common platforms and cloud information storage, leading to the need to protect the data contained in them, and therefore, to have a formal national cybersecurity strategy.

Brazil, India and South Africa are experiencing difficulties in the development of the information and communication infrastructure, which is currently rated at 0.35–0.65. The construction of fiber-optic networks could become a promising area of economic cooperation within the BRICS.[79]

The Russian Federation is the leader in terms of the level of human capital development, with a rating of 0.88. The remaining member countries need to make efforts to eliminate the digital divide between certain territories and segments of the population. International educational and research programs, which are an integral part of cybersecurity cooperation, can be helpful in this regard.

A detailed study of the e-governments of these countries leads us to the conclusion that all of the countries have made significant achievements in the provision of online public services (from 0.9 to 0.74). According to this indicator, the BRICS member

[79] Stacia Lee, *International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable*, University of Washington (January 2016) (Feb. 2, 2023), available at https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/.

countries are in the top twenty nations worldwide. The government systems of the countries studied are highly integrated with digital platforms and cloud storage systems, which makes them vulnerable to cyberthreats. These observations allow us to conclude that all of the BRICS member countries are highly interested in the formation of a common, well-regulated state cybersecurity system.

However, after a thorough study of the Global Cybersecurity Index (2018), we found that countries with government regulation have a higher cybersecurity level (Russia, China). This level directly depends on the degree of responsibility assumed by the state. Countries with insufficiently centralized cyber defense systems are lower in the rating (Brazil, South Africa, India) and are often affected by cyberattacks. As a result, India was forced to apply government regulation of cyberspace, which increased its effectiveness. We therefore come to this conclusion that there are objective grounds for strengthening state control over cybersecurity and hope that the positions of the BRICS member countries can be brought closer together.

According to our study of the bilateral agreements on cybersecurity cooperation of the BRICS member countries, we concluded that there are common areas for cooperation. These areas include:

- Educational projects that enhance human potential.
- Joint applied research.
- Joint actions to close the digital divide and develop broadband access networks in all countries of the bloc.
- Unification of legislation of the member countries on the criminalization of unlawful acts in cyberspace.

We believe that in order to move to a strategic level of interaction and coordinate the actions of the BRICS member countries in the international arena, a mixed intergovernmental committee for cybersecurity cooperation should be created. This committee will serve as an executive body for the preparation and execution of the following events,

- Exchange of information and best practices in combating cybercrime.
- Development of an integrated digital platform of the BRICS member countries to exchange data on cyber incidents in the financial sector, best practices and regulatory experience in information security.
- Regular publication of the Compendium of Best Practices on the Supervision and Control of Information Security Risks as well as its publication on a digital platform.
- Implementation of bachelor's and master's cybersecurity programmes within the BRICS Institute.

In addition, the current state of world affairs requires that the BRICS countries consolidate their position in the field of cybersecurity. The first step could be to hold a video meeting among representatives of the Group of Five Countries in charge of security issues to adopt a joint memorandum.

References

Bruijn H. & Janssen M. *Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies*, 34(1) Government Information Quarterly 1 (2017). https://doi.org/10.1016/j.giq.2017.02.007

Burak A. & Barış D. *Analysis of the Cyber Security Strategies of People's Republic of China*, 14(28) Güvenlik Stratejileri Dergisi (Journal of Security Strategies) 1 (2018). https://doi.org/10.17752/guvenlikstrtj.495748

Chandel S. et al. *The Golden Shield Project of China*: *A Decade Later an In-depth Study of the Great Firewall*, in 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 111 (2019). https://doi.org/10.1109/CyberC.2019.00027

Khanna P. *State Sovereignty and Self-Defence in Cyberspace*, 5(4) BRICS Law Journal 139 (2018). https://doi.org/10.21684/2412-2343-2018-5-4-139-154

Kortjan N. *A Conceptual Framework for Cyber Security Awareness and Education in South Africa*, 52(1) South African Computer Journal 29 (2014). https://doi.org/10.18489/sacj.v52i0.201

Markopoulou D. et al. *The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation*, 35(6) Computer Law and Security Review 1 (2019). https://doi.org/10.1016/j.clsr.2019.06.007

Mawela T. et al. *E-Government Implementation: A Reflection on South African Municipalities*, 29(1) South African Computer Journal 147 (2017). https://dx.doi.org/10.18489/sacj.v29i1.444

Mohanty S.P. et al. *On the Design of a Youth-Led, Issue-Based*, *Crowdsourced Global Monitoring Framework for the SDGs*, 11(23) Sustainability (Article 68399) (2019). https://doi.org/10.3390/su11236839

Niekerk B.V. *South Africa and the Cyber Security Dilemma*, 18(2) Journal of Information Warfare 96 (2019). https://doi.org/ 10.23962/10539/23573

Nikitin E. & Marius M. *Unified Digital Law Enforcement Environment – Necessity and Prospects for Creation in the "BRICS Countries"*, 7(2) BRICS Law Journal 66 (2020). https://doi.org/10.21684/2412-2343-2020-7-2-66-93

Samion N.A. & Mohamed A. *Innovation of National Digital Identity: A Review*, 9(1.2 Special Issue) International Journal of Advanced Trends in Computer Science and Engineering 151 (2020). https://doi.org/10.30534/IJATCSE/2020/2391.22020

Song Z. et al. *China's Prefectural Digital Divide: Spatial Analysis and Multivariate Determinants of ICT Diffusion*, 52 International Journal of Information Management (Article 102072) (2020). https://doi.org/10.1016/j.ijinfomgt.2020.102072

Stevens T. *Global Cybersecurity: New Directions in Theory and Methods*, 6(2) Politics and Governance 1 (2018). https://doi.org/10.17645/pag.v6i2.1569

Vakulyk O. et al. *Cybersecurity as a Component of the National Security of the State*, 9(3) Journal of Security and Sustainability Issues 775 (2020). https://doi.org/10.9770/JSSI.2020.9.3(4)

Yuan L. et al. *Evaluating the Readiness of Government Portal Websites in China to Adopt Contemporary Public Administration Principles*, 29(3) Government Information Quarterly 403 (2012). https://doi.org/10.1016/j.giq.2011.12.009

Information about the authors

Oksana Ovchinnikova (Chelyabinsk, Russia) – Associate Professor, Department of Judicial and Law Enforcement Activities, Institute of Law, South Ural State University (National Research University) (47a Elektrostalskaya St., Chelyabinsk, 454038, Russia; e-mail: ovchinnikova-ov@yandex.ru).

Niteesh Kumar Upadhyay (Nodia, India) – Associate Professor, Symbiosis Law School, Noida Campus, Symbiosis International (Deemed University) Pune (Block A, 47/48, Sector-62, Noida, 201301, India; e-mail: niteesh_marshal@yahoo.co.in).