POLICY BRIEF

54 / 2024

BRICS Expansion and Prospects for BRICS Cooperation in the Digital Economy

Alexander Ignatov

RIAC
Russian International
Affairs Council

RUSSIAN INTERNATIONAL AFFAIRS COUNCIL

Author:
Alexander Ignatov, Ph.D. in Political Science

Editors:
Svetlana Gavrilova, Ph.D. in History (Lead Editor), **Konstantin Sukhoverkhov**, **Katerina Trotskaya**, **Daniil Rastegaev** (Publishing Editor)

The Russian International Affairs Council (RIAC) is a non-profit organization focused on research in the field of international relations and developing practical recommendations for the benefit of Russian government bodies, business, NGOs and other organizations engaged in foreign policy activities. The Council was established by the decision of its co-founders in accordance with the order of the President of the Russian Federation, dated February 2, 2010 № 59-rp "On the Establishment of the Non-Commercial Partnership 'Russian International Affairs Council'."

RIAC is one of the leading national think tanks, exploring more than 20 research areas. The Council's expertise is in demand by Russian specialized agencies, the academic community, national and international business.

RIAC Board of Trustees is chaired by Sergey Lavrov, Minister of Foreign Affairs of the Russian Federation. RIAC President, Corresponding Member of the Russian Academy of Sciences Igor Ivanov, served as Minister of Foreign Affairs of Russia in 1998-2004 and Secretary of the Security Council of the Russian Federation in 2004-2007. The Council's Director General is Ivan Timofeev. The Research Advisor of the Council is Andrei Kortunov.

FOUNDERS

Ministry of Foreign Affairs of the Russian Federation

Ministry of Education and Science of the Russian Federation

Russian Academy of Sciences

Russian Union of Industrialists and Entrepreneurs

Interfax News Agency

The opinions expressed in this policy brief reflect solely the personal views and analytical outlook of the author and do not necessarily represent the views of the Russian International Affairs Council Non-Profit Partnership.

The full text of the policy brief is available on RIAC's website.

Cover photo: RIA Novosti / Alexei Maishev

BRICS Expansion and Prospects for BRICS Cooperation in the Digital Economy

Introduction

The development of digital technologies is transforming the structure of world politics, fundamentally changing the balance of power in the international arena. Traditional components of state power — armed forces, economic, scientific and demographic potential, the ability to establish an acceptable model of behavior for other actors in international politics, etc. — are undergoing profound changes. It is difficult to imagine a modern armed conflict without the ability of using digital technologies to inflict damage on adversaries, including in information and psychological warfare. Entire sectors of the economy, especially real production, are adopting new trends as they harness advanced solutions in the field of the Internet of Things, Big Data and artificial intelligence. The digital revolution has brought the world together into a single information space or network, building relations between people and societies all over the planet in a much easier and efficient way. In the eyes of techno-optimists, the key to solving global problems of humanity — hunger, inequality, poverty, adaptation to climate change, prevention of new pandemics, etc. — lies in the development of digital economy.[1]

However, the benefits of the growing digital economy are inevitably associated with new threats. Information globalization has not only brought continents and people closer together, but has also triggered the rise of international cybercrime, the unprecedented spread of terrorist or extremist ideas and narratives, adding cyberattacks to the list of threats to international security, as well as cyberattacks capable of causing damage comparable in scale to the consequences of using the weapons of mass destruction.

Another characteristic of modernity is the existence of rules and norms that can smooth out mounting contradictions and make the behavior of actors in international politics more predictable. However, these rules are often formulated too late, failing to keep pace with the transformation of threats. Despite the fact that all states are confronted by global challenges, the most vulnerable are the countries of the so-called global majority.

Despite the positive developments of recent decades, a substantial part of the world's population, as well as the sovereign states that represent them (both individually and in alliances), still have relatively little or no influence shaping the new rules and structures of global governance in the digital economy.

Every challenge sets the stage for countermeasures. In the context of globalization, an effective response can only be formulated through collective effort. The extent to which this response will meet the criterion of fairness and to the extent to which the interests of all involved parties will be truly considered depends directly on the latter's activity on the international arena. In the absence of constructive participation in international negotiations, for many states in the non-Western world,[2] BRICS seeks to represent and promote their interests, stating this as one of its strategic objectives.

BRICS has successfully fulfilled its role as an international negotiating platform. For over a decade of its existence, member states have made hundreds of decisions on key issues on the agenda.[3] The most general list of issues discussed within

ABOUT THE AUTHOR
Alexander Ignatov — Ph.D. in Political Science, Senior Researcher at the International Institutes Research Center at the Institute of Applied Economic Policies, RANEPA.

[1] For example, see: Lechman E., Popowska M. Harnessing digital technologies for poverty reduction. Evidence for low-income and lower-middle income countries. Telecommunications Policy. 2022. Vol. 6. No. 6.; Neto O.L., Wyl V.V. Digital Transformation of Public Health for Noncommunicable Diseases: Narrative Viewpoint of Challenges and Opportunities. JMIR Public Health Surveill. 2024. Vol. 10; Whitelaw S. et al. Applications of digital technology in COVID-19 pandemic planning and response. The Lancet Digital Health. 2020. Vol. 2. No. 8. P. 435-440.

[2] For example, see research on the reasons for low activity of African nations in negotiations on the WTO platform: The E-Commerce Negotiations within the WTO. Understanding non-participation // National board of trade Sweden.
URL: https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2023/the-e-commerce-negotiations-in-the-wto.pdf

[3] See a more detailed review of achievements during the initial decade of BRICS operations: Larionova M.V. et al. Ten Years of BRICS: What's Next? Moscow: Delo Publishing House, 2020, P. 98.

the framework of the association includes dozens of topics ranging from macroeconomic policy to countering extremism and terrorism, as well as the development of ICT and digital economy. Numerous multilateral cooperation mechanisms have been created within the BRICS framework, the New BRICS Development Bank has been established and is operating, cooperation in the field of security and humanitarian exchanges is also developing.

Dozens of applications to join the BRICS prove the demand for the organization association and the international agenda it promotes.[4]

Radical BRICS membership enlargement is a stress test for any international institution,[5] fraught with the possible loss of its established identity and internal synergies, which is especially important in the joint promotion of multilateral initiatives. This study seeks to answer the question of what opportunities and challenges the BRICS enlargement may arise, as well as unlock BRICS potential in managing the development of the digital economy.

BRICS From Yekaterinburg to Johannesburg: Achieved Progress

Prior to enlargement, BRICS's main successes in the multilateral governance of the digital economy was largely due to Russia and China's leadership, whose initiatives in most areas are supported by Brazil, India and South Africa. Precisely since Russia's 2015 BRICS presidency, the ICT development agenda been formalized as an independent area of cooperation.

Previously, this issue was discussed on the margins of the Ministers of Science meetings. A symbolic start to this process was the meeting of BRICS Communications Ministers in Moscow, where the first joint declaration on cooperation was adopted.[6]

BRICS cooperation on digital growth distinguishes itself when it comes down its different conditions for the development of national digital economies, hence the positioning of priority issues for multilateral discussion. In terms of key indicators – the share of the population actively using the internet, the share households with a personal computer, the spread of digital skills, as well as assessments regarding the size of the digital market and the adequacy of measures to counter cyberthreats, etc. — the "old" BRICS leaders are Russia and China.[7] Digital infrastructure development remains a common priority for the "founding five", but their approaches differ in the details. In the case of China, India, South Africa and Brazil, developing digital infrastructure in economically backward regions, also characterized by relatively low population incomes, is at the forefront. Russia also considers developing a regional infrastructure, but it is more concerned about assisting remote and sparsely populated areas without aggravating low incomes.[8]

Even though the threat of major foreign company monopolization over the national platform services market is recognized by all BRICS nations, only Russia and China have implemented a response commensurable with the scale of the threat via countermeasures by local regulators driven by relevant legal norms.

Russia has adopted the Concept of State Regulation of Digital Platforms and Ecosystems[9] and published industry standards regulating certain

[4] More than 40 countries would like to join BRICS and 6 countries have already received a formal invitation to join // Rossiyskaya Gazeta. 22.09.2023. URL: https://rg.ru/2023/09/22/strategicheskij-prioritet.html

[5] For example, see the Shanghai Cooperation Organization enlargement case: Muratbekova A. The Crisis of SCO Identity: What's Next? // The Bulletin of International Organizations. 2019, Vol. 14. P. 138-160.

[6] Communique of BRICS Ministers of Communications on the outcomes of the meeting "Expansion of Cooperation in the Field of Communications and ICTs" // BRICS. URL: http://en.brics2015.ru/load/637860

[7] See information on several other indicators: BRICS Joint Statistical Publication 2023 // Rosstat. URL: https://rosstat.gov.ru/storage/document/document_statistic_collection/2024-01/15/BRICS%20Joint%20Statistical%20Publication-2023 (1).pdf. Also see: Ignatov A.A. Digital Economy in BRICS: the Outlook for Multilateral Cooperation // The Herald of International Organizations. 2020, Vol. 15. No 1. P. 31-62.

[8] See: Ignatov A.A. BRICS in Internet Control. Moscow: Infra-M, 2024. P. 104-108.

[9] The concept of state regulation of digital platforms and ecosystems // Ministry of Economic Development of the Russian Federation. URL: https://www.economy.gov.ru/material/departments/d31/koncepciya_gos_regulirovaniya_cifrovyh_platform_i_ekosistem/

aspects of interaction between digital market participants.[10] In 2020-2021, China developed and adopted the Guidelines on Antimonopoly Regulation in the Platform Economy,[11] introduced special provisions on the Law on Countering Monopolies to address the situation in the digital platform services market, as well as published Guidelines on the Classification of Online Platforms.[12]

Brazil, India and South Africa have a similar initial process, i.e. the first stage of discussing requirements for of the localization of user data, moderation of distributed content, notification of pending mergers and acquisitions, etc., or attempting to apply existing legislation to regulate the market situation. In the Brazilian Parliament, Bill 2.768 on the regulation of online platforms — covering only large, predominantly foreign platforms — has been under discussion since 2022.[13] In India, the Digital Competition Bill has been tabled for discussion in 2023.[14] The Bill proposes to establish new rules to regulate a few large digital platforms — "systemically important digital enterprises" based of revenue generated. Content-wise, the Bill is an attempt to introduce ex-ante regulations, which adhere to international best practices. Yet, according to government experts, this may be counterproductive in India as an emerging economy. South Africa's legal system does not have a specific law to regulate online platforms, which, combined with an imperfect institutional structure, leads to a fragmented regulatory system and ineffective remedial measures for market competition. Thus, the Competition Commission of South Africa has met the requirements for online platform operators to improve the competitive situation in the market in only a few cases out of the entire list of problems identified in the market study.[15]

Thus, attempts to use advanced international experience — for example, modeling after the EU General Data Protection Regulation[16] — do not always meet national conditions, and BRICS as a group has yet to find consensus in this area. The approaches of the "founding five" to international information security also differ.[17] Russia and China demonstrate leadership regarding the protection of the national information space.

The approaches of the "founding five" to international information security also differ.[18] Russia and China demonstrate leadership in relation to the protection of the national information space. These countries prioritize "digital sovereignty" in their policies, ensuring the independence of their states in the digital realm and maintaining the ability to independently implement information policy at home and in the international arena,[19] explaining the rigidity in the requirements for the localization of user data and the withdrawal of undesirable materials containing mainly extremist and terrorist narratives from circulation. Most importantly, along with the legal apparatus, Russia[20] and China[21] probably possess the richest experience in implementing these provisions in everyday practice. For example,

[10] For example, see: The Standards for Interaction Between Marketplaces and Vendors of Goods (Edition No. 3) // The Association of Internet Retail Companies. 2024. URL: https://admin.akit.ru/wp-content/uploads/2024/08/240816-Standarty_MP_i_prodavtsy_redaktsiya_-_3.pdf ; Standards for Interaction Between Marketplaces and Owners of Orders Pick-up Points // Normative Contour. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=458483

[11] Anti-monopoly regulation of digital platforms in China // CeCo.
URL: https://centrocompetencia.com/anti-monopoly-regulation-of-digital-platforms-in-china/

[12] China's new platform guidelines // Data protection and digital competition.
URL: https://www.ianbrown.tech/2021/11/01/chinas-new-platform-guidelines/

[13] Chiarini T. et al. Regulation of markets mediated by digital platforms in Brazil // Center for Research on Science, Technology and Society. 2023.
URL: https://www.ipea.gov.br/cts/en/all-contents/articles/articles/381-regulation-of-markets-mediated-by-digital-platforms-in-brazil-an-open-discussion

[14] MCA invites public comments on Report of Committee on Digital Competition Law and Draft Bill on Digital Competition Law // Press Information Bureau.
URL: https://pib.gov.in/PressReleasePage.aspx?PRID=2013947

[15] See: Ignatov A.A. Regulation of Digital Platforms in BRICS: Priorities and South Africa's Experience // The Bulletin of International Organizations. 2024, Vol. 19. No. 2. P. 161-182; also see research done by experts of the World Bank: Al-Dahdah E. et al. South Africa — Digital Economy Diagnostic // World Bank Group. 2024.
URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/464421589343923215/south-africa-digitaleconomy-diagnostic

[16] General Data Protection Regulation (GDPR) of the European Union // GDPR Text. URL: https://gdpr-text.com/ru/

[17] See: Zinovieva E.S., Shitkov S.V. BRICS on the Way Towards Acquiring Digital Sovereignty? // The Problems of National Strategy. 2024. No. 2 (83). P. 144-183.

[18] See: Zinovieva E.S., Ignatov A.A. Digital Sovereignty on the BRICS Agenda // RIAC. 24.01.2024.
URL: https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/

[19] See Federal Law No. 139-FZ dated July 28, 2012 "On Entering Amendments to Federal Law 'On Protecting Children from Information Causing Harm to Their Health and Development' as well as certain legislative acts of the Russian Federation on limiting the access to illegal information in the Internet" // Consultant Plus. URL: https://www.consultant.ru/document/cons_doc_LAW_133282/

[20] See: Provisions on the Governance of the Online Information Content Ecosystem // China Law Translate. URL: https://www.chinalawtranslate.com/en/provisions-on-the-governance-of-the-online-information-content-ecosystem/; Also see: 2016 Cybersecurity Law // China Law Translate.
URL: https://chinalawtranslate.com/en/2016-cybersecurity-law/

[21] Roskomnadzor has blocked more than 23,000 pages of ISIS propaganda in Russian // Interfax. 24.03.2017. URL: https://www.interfax.ru/russia/555127

the competent Russian agency, Roskomnadzor, has ensured the blocking of thousands of online pages containing extremist propaganda of ISIS, an organization which is banned in Russia.[22] Every year Roskomnadzor takes decisions to block thousands of Internet resources disseminating illegal information.[23] There are different estimates regarding the scale of blocking undesirable materials in China. Thus, according to a study conducted in 2021, about 350 thousand Internet resources are inaccessible for Internet addresses in China, but it is possible that this number is significantly higher than was noted in the study.[24] Before BRICS enlargement, only Russia and China were considered to have a high potential for using digital technologies for attacking purposes.

The closest partner to the Russia and China "duo" in terms of declared priorities is India, which is taking measures to exclude certain content from circulation, including the activities of separatist groups. It has been reported that over 55,000 websites, mostly independent news outlets, were blocked in India between 2015 and 2023. About half of these cases involve provisions of the Information Technology Act. A distinctive behavior pattern of the Indian authorities is the absence of prior notification demanding the removal of unwanted content. It is reported that blocking decisions are almost impossible to challenge because the orders of the competent authorities (if any, which is not directly stated in the investigation) are not publicly announced. A recent example is the case of Kashmirwalla, a website covering the situation in the state of Jammu and Kashmir, which suddenly became no longer available in India.[25]

Brazil and South Africa differ from its other partners both in terms of declared priorities and established practices in the realization of digital sovereignty. These states can be classified as supporters of the "soft concept" of digital sovereignty, which in practice means that their approach to digital security does not prioritize the regulation of content distributed online, the latter being typical positions taken by Russia, China and India.[26]

The transforming discussion within BRICS on information security over the past five to seven years has been influenced by Russia and China's supportive proposal. Moscow, which pioneered the international discussion on information security at the UN, has succeeded in expanding the BRICS multilateral dialogue on digital security to include counterterrorism and extremism, documented in the BRICS Anti-Terrorism Strategy of 2020[27] and its Implementation Plan of 2021.[28] Russian initiatives are supported by China both within BRICS and in the international arena. The shared membership in the Shanghai Cooperation Organization, including India from the Old Five, is also a point of convergence, and a security cooperation agenda, including in the digital space, has been developing for many years. Other BRICS partners support the proposed initiatives, but have not put forward any new solutions of their own.

In other words, even taking into account the obvious success of multilateral diplomacy, it should be noted that BRICS cooperation on digital development, although nominally covering a wide range of issues, is really effective either in areas where the interests of the member states converge without pronounced contradictions (infrastructure development) or in areas where one or more countries have a pronounced leadership potential sufficient to overcome possible disagreements (Russia's position on international information security). Effective cooperation in other areas, such as the regulation of digital platforms, is hampered by obvious differences in the maturity of local markets.

[22] Roskomnadzor has blocked over 170,000 pages with illicit content in 2024 // TASS. 17.04.2024. URL: https://tass.ru/obschestvo/20568701

[23] See: Cimpanu C. China's Great Firewall is blocking around 311k domains, 41k by accident // The Record. 2021. URL: https://therecord.media/chinas-great-firewall-is-blocking-around-311k-domains-41k-by-accident ; Hoang N.P. et al. How Great is the Great Firewall? Measuring China's DNS Censorship // ArXiv. 2021. URL: https://arxiv.org/abs/2106.02167

[24] Website blocking in India: One arrow for all // Advox. URL: https://advox.globalvoices.org/2024/08/19/website-blocking-in-india-one-arrow-for-all/

[25] For more, see: Zinovieva E.S., Ignatov A.A. BRICS in a Global ICT Security Regime // International Processes. 2023. Vol. 21. No. 4 (75). P. 104-132.

[26] Anti-Terrorist Strategy of BRICS // Official website of Russian Federation's chairmanship in BRICS.
URL: https://brics-russia2020.ru/images/114/81/1148163.pdf

[27] BRICS Counter-Terrorism Action Plan // BRICS India 2021. URL: https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-52.pdf

[28] Sebekin S.A. The Role of Shanghai Cooperation Organization and BRICS in Ensuring International Information Security under an Ongoing Conflict in Ukraine // Russian-Chinese Studies. 2022. Vol. 6. No. 4. P. 279-281.

BRICS + 5: An Opportunity or a Challenge?

It is impossible to ignore the complexity of the challenge posed by BRICS permanent member enlargement. Integrating new members into the established negotiation practices of BRICS is necessary to ensure their active involvement in the work of the mechanisms already in place. The issue of new member state priorities in this area requires further clarification.

The five new BRICS member countries have even more differences in their assessments of digital development and their position in the emerging system of control over the development of the digital economy (Table 1).

Table 1. Digital Development Indicators of the New BRICS Countries

Country	Internet users, % of the population	Mobile phone ownership, % of the population	3G / 4G Cellular network coverage	Cost of broadband Internet connection, % of GNP per capita	Traffic via mobile networks, GB (inside the country)
Ethiopia	19.4 (2022)	58.3 (2016)	98.5 / 33 (2022)	12.1 (2023)	19.8 (2022)
Egypt	72.2 (2022)	97,4 (2022)	99.8 / 98 (2023)	2.4 (2023)	52.9 (2023)
Iran	81.7 (2022)	72.4 (2021)	92 / 91 (2023)	0.17 (2023)	129 (2023)
Saudi Arabia	100 (2023)	100 (2023)	100 / 100 (2023)	2.99 (2023)	531 (2023)
UAE	100 (2023)	100 (2023)	99.8 / 98.5 (2023)	0.44 (2023)	172 (2023)

Source: ITU DataHub[29]

For example, the position of countries such as Saudi Arabia and United Arab Emirates, is differs than that of Ethiopia. The former two represent well-established, developed markets of digital products and services, where governments can choose from among the constantly expanding pool of international regulatory practices, whose implementation on the local level will most likely allow them to achieve the expected positive effects. As for Ethiopia, its primary focus is the development of its basic infrastructure,[30] dissemination of elementary digital skills and protection from an avalanche of digital vulnerabilities, including those caused by the low digital literacy of consumers regarding services provided by financial online intermediaries. Iran notably stands out among other member states: this country has been developing for many years under immense sanctions pressure, restricting the presence of major overseas platforms in the local market. Not every proposed national counterpart is actively sought after by Iranian consumers. Egypt is one of the biggest digital markets in the region, openly positioning itself in international affairs. Nevertheless, digital market regulation regimes, as well as the national turnover of user data, require quality revision to adapt to modern-day realities.

Now to consider the above-mentioned, as well as other, distinctive characteristics of the positions of the five new BRICS members in more detail. Ethiopia is going through the stage of intensive digital growth as the share of its residents using the Internet and broadly speaking digital technologies on a regular basis continues to rise. In Ethiopia this indicator is estimated at the level of 19.4% which is lower than the average index for African countries (37%).[31] Rampant cybercrime is typical of this development stage — just recently Ethiopia was among the five countries in the world where the risk of encountering a case of malicious exploitation of internal vulnerabilities in popular software was the highest.[32] According to Ethiopia's own estimates, the potential damage of reflected cyberattacks alone could have amounted to about $330 million in 2022-2023. The total number of reported cases exceeded

[29] ITU DataHub. URL: https://datahub.itu.int/

[30] For example, see: The Strategy of National Digital Development: Digital Ethiopia 2025: Empowering the nation in the digital economy // Resilient. 11.04.2024. URL: https://resilient.digital-africa.co/en/blog/2024/04/11/digital-ethiopia-2025-empowering-the-nation-in-the-digital-economy/

[31] Africa's Internet use doubles in decade despite high costs (report) // Ecofin Agency. 27.02.2024. URL: https://www.ecofinagency.com/telecom/2702-45230-africas-internet-use-doubles-in-decade-despite-high-costs-report

[32] Microsoft Security Intelligence Report // Microsoft. URL: https://info.microsoft.com/SIRv24Report.html

18,000 by the end of 2023 — marking a fourfold increase from the previous period (4,000 at the end of 2022).[33] The International Telecommunication Union ranked Ethiopia 115th out of 182 assessed states in its cybersecurity ranking.[34]

In the case of Ethiopia, estimating the size of the domestic market for digital goods and services is a daunting challenge; hence the impossibility of drawing valid conclusions about the competitive situation in this sphere. Available estimates cautiously put the share of ICT-related sectors in the country's GDP at 2%,[35] which is below the East African average. Other expert opinions suggest that the entire digital segment of the country's economy is a collection of several hundred (up to 600) small IT companies.[36] The largest representatives of local digital businesses, mainly online marketplaces such as Qefira, Engocha and Jiji, are characterized by a reach of 50-150 thousand special visitors per month, with Google taking the main revenue from advertising and user interactions.[37] It is reported that the local counterpart of Google's search engine, Yahoonoo, whose distinctive feature was better at handling the Amharic language, does not currently work. The regulatory system for online platforms in Ethiopia appears fragmented, providing insufficient competition protection for local businesses with too few resources to compete with foreign companies.

The situation is somewhat different in another important aspect of digital development — user data management. Ethiopia has borrowed the experience of the European General Data Protection Regulation (GDPR), with which the Data Protection Regulation[38], in force since April 2024, shares definitions, lists of rights and obligations of data subjects and data operators, as well as provisions on cross-border data transfers. Experts[39] highlight the difference in the implementation of the Ethiopian Regulation's provisions and the European GDPR in terms of the obligation to eliminate personal data collected at the request of data subjects. It is considered that the GDPR does not directly require data controllers to ensure the deletion of data-by-data handlers, which is directly required in the Regulation's provisions.

Ethiopia is not one of the active actors in the emerging digital economy governance mechanisms. This is largely due to a set of challenges common to most African countries, in particular, the lack of competencies and resources for continuous participation in multilateral discussions. This is evident in the WTO negotiations on digital trade regulation. Ethiopia, together with other African states, is part of the so-called African Group, which allows countries to declare their interests formally at the international level, while at the same time "dissolves" its local specifics into a middle-ground collective position. Ethiopia's bilateral arrangements with US business,[40] China,[41] India,[42] the UK,[43] as well as the EU[44] do not directly address digital growth and are often focused on basic development issues. The implementation of these projects is likely to have a catalytic effect on digital growth by increasing the prosperity of the local population and, as a result, increasing demand for digital products and services, creating an incentive for the development of digital industries.

[33] INSA saves 19 billion birrs in 9 months // INSA Ethiopia. URL: https://insa.gov.et/sv/web/en/w/insa-saves-19-billion-birrs-in-9-months

[34] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[35] Ethiopia's digital economy is blooming, but needs investment // ECDPM. 21.11.2022.
URL: https://ecdpm.org/work/ethiopias-digital-economy-blooming-needs-investment

[36] Review — Ethiopia's Digital Economy Report // Shega. URL: https://shega.co/post/review-ethiopias-digital-economy-report/

[37] Review of the Top 3 Online Marketplaces in Ethiopia: Engocha // Shega.
URL: https://shega.co/post/review-of-the-top-3-online-marketplaces-in-ethiopia-engocha/

[38] Personal Data Protection Proclamation 1321/2024 // BonelliErede. 07.05.2024.
URL: https://www.belex.com/en/case_study/personal-data-protection-proclamation-1321-2024/

[39] Ethiopia: General overview of Ethiopia's first personal data protection proclamation in light of the EU GDPR // DataGuidance.
URL: https://www.dataguidance.com/opinion/ethiopia-general-overview-ethiopias-first-personal

[40] Microsoft Chooses Ethiopia as One of Africa New Digital Development Programme // Fana BC.
URL: https://www.fanabc.com/english/microsoft-chooses-ethiopia-as-one-of-africa-new-digital-development-programme

[41] See: Interview: BRI cooperation with China transforms Ethiopian lives for better // Belt and road portal. 26.03.2024.
URL: https://eng.yidaiyilu.gov.cn/p/0SAV3Q82.html; Also, see: Chinese investment hailed as essential driver of Ethiopia's economic development // Xinhua. 23.06.2024. URL: https://english.news.cn/africa/20240623/f12d2b70246f41d3baac0a315bd5f0c8/c.html

[42] Tsukanov L.V. Technological Renaissance in Sub-Saharan Africa: Challenges and Opportunities for Russia // PIR-Centre, 2024.
URL: https://pircenter.org/editions/37-2024-tehnologicheskij-renessans-v-afrike-juzhnee-sahary-vyzovy-i-vozmozhnosti-dlja-rossii/

[43] UK — Ethiopia development partnership summary, July 2023 // UK Government. 17.07.2023.
URL: https://www.gov.uk/government/publications/uk-ethiopia-develpment-partnership-summary/uk-ethiopia-development-partnership-summary-july-2023#key-programmes

[44] EU, OACPS and UNCDF to Launch a New Programme on Digital Finance in Ethiopia // UNCDF.
URL: https://www.uncdf.org/article/6852/eu-oacps-and-uncdf-to-launch-a-new-programme-on-digital-finance-services-in-ethiopia

Among African countries, ***Egypt*** has one of the largest digital markets, characterized by relatively high rates of access to digital infrastructure, both in urban and rural areas, compared to other developing nations. According to statistics, more than 70% of the population in Egypt regularly use the Internet, with at least 70% of households owning a personal computer. Broadband infrastructure allows for the average data transfer speed to be 10 Mbps.[45]

To develop a national legal framework for user data management, Egypt has adopted the experience of the European General Data Protection Regulation. Egypt's 2020 Data Protection Law[46] uses similar definitions to the GDPR. The law is extraterritorial in nature, while cross-border transfers of user data require authorization from the competent authority and are only allowed in jurisdictions whose status is determined to be reliable by the national regulator.

Amid the proliferation of internet access in Egypt, there has been a massive increase in the number of cyber incidents recorded. The growth is particularly rapid in the financial technology sector, with an increase in attempts to gain unauthorized access to banking systems by 186% between 2022 and 2023. At the same time, the number of incidents involving the theft of user data through phishing links increased by nearly 50%.[47] Within its regional group, Egypt ranks 4th in digital preparedness, behind Saudi Arabia, the UAE and Oman.[48]

Egypt implements a rather rigorous approach to regulating online media. According to the provisions of the 2018 Media and Press Regulation Law49, all online information platforms with an audience of more than 5,000 users are categorized as media outlets and are obliged to fulfill the requirements to counter the spread of fake news and inaccurate information. Launching a page in the Egyptian internet domain requires a special state license. The Law on Countering Cybercrime and the ICT Misuse of 201850 obliges telecommunications companies to retain user data for 180 days and provide law enforcement agencies access to counter extremist and terrorist propaganda among youth. Blocking internet resources on suspicion of disseminating prohibited information can take place on a pre-trial basis. The Egyptian Ministry of Foreign Affairs has been instructed to conclude agreements with foreign countries to block internet resources that disseminate unlawful information. Egypt, Saudi Arabia and the US have become founding members of the Etidal Global Center for Countering Extremist Ideology.[51]

The Egyptian digital market is noted for a strong presence of foreign companies and platforms, which are leading in many segments: search engines, social media, and food delivery. Currently, no reports of extensive market competition studies conducted or being conducted by the local regulator have been found. In the absence of a specialized law on digital platforms, threats of market monopolization by foreign companies are managed in accordance with the 2005 Competition Act.[52] UNCTAD experts argue that the local regulator has difficulties in determining the market position of digital companies and recommend numerous amendments to the current law to combat abuses of the market, such as failure to maintain interoperability of platforms and uneven access to information by different users.[53]

Egypt is quite active in the international arena. Its representatives participated in the UN Group of Governmental Experts on International Information Security from 2012 to 2017, and made a number of comments on the mandate, structure and content of the ongoing Regular Inter-Institu-

[45] Digital Development Dashboard // ITU. URL: https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

[46] Egypt — Data Protection Overview // DataGuidance. URL: https://www.dataguidance.com/notes/egypt-data-protection-overview

[47] 49% increase in phishing attacks in Egypt during 1Q 2023: Kaspersky // Daily News Egypt. 07.05.2023.
URL: https://www.dailynewsegypt.com/2023/05/07/49-increase-in-phishing-attacks-in-egypt-during-1q-2023-kaspersky/

[48] Global Cybersecurity Index 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[49] Law No. 180 of 2018 on Press, Media and the Supreme Council for Media Regulation, Egypt // WIPO Lex.
URL: https://www.wipo.int/wipolex/en/legislation/details/19960/. Also see: Egypt targets social media with new law // Reuters. 18.07.2018.
URL: https://www.reuters.com/article/world/egypt-targets-social-media-with-new-law-idUSKBN1K720I/

[50] Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Egypt // WIPO Lex. URL: https://www.wipo.int/wipolex/en/legislation/details/19959

[51] Etidal and Telegram Combat Extremist Propaganda by Removing 18 Million Extremist Content for the Second Quarter of 2024 // Etidal. 02.07.2024.
URL: https://etidal.org/en/etidalandtelegramcombatextremistpropagandabyremoving18millionextremistcontentforthesecondquarterof2024/

[52] Law No. 3 of 2005 Promulgating the Law on the Protection of Competition and the Prohibition of Monopolistic Practices // WIPO Lex.
URL: https://www.wipo.int/wipolex/en/legislation/details/7409

[53] Voluntary peer review of competition law and policy of Egypt: Overview // UNCTAD.
URL: https://unctad.org/system/files/official-document/ciclpd75_en.pdf

tional Dialogue Mechanism on Security in the Use of ICTs.[54] Egypt participates in WTO negotiations on the regulation of e-commerce and supports the 1998 work program.[55] At Egypt's suggestion, provisions related to managing the development of artificial intelligence were added to the African Union's working agenda.[56]

Iran has achieved a relatively high level of digital development compared to countries with similar wealth. The share of Iranians who use the Internet is estimated at 80%, with about 92% of the entire population residing in areas covered by 4G wireless communication networks.[57] Internet traffic is mainly transmitted via mobile devices. Iran is behind countries with comparable levels of development in terms of broadband data transmission. The national digital market is estimated at USD 24.6 billion with a possible further growth to USD 29 billion by 2029. The high share of young people (under 35) creates prerequisites for the development of digital sectors due to the expected growth in demand.[58]

Iran pursues the policy of potentially using cyberspace for conducting special operations, but in the meantime Iran itself is facing problems with a rebuff of cyberthreats. According to data, about 150 million users of electronic goods and services in Iran suffered because of data leakage. This means that each active user of Internet services in Iran could become a victim of data leakage at least twice over the past year.[59]

In regulating the circulation of user data and the operation of online platforms, Iran is guided by existing laws[60] that have yet to contain special provisions reflecting, for example, the special conditions for competition in the digital market. This leaves certain categories of user data unprotected, i.e. unauthorized access to them may not be considered a crime. Even if there are no major foreign players in the market, there is a threat of monopolization and abuse of market leadership by domestic companies.

Iran's tough stance on digital content regulation is well known. Competent authorities block access to many popular apps and platforms and demonstrate high potential in terms of limiting internet traffic. For example, during the 2019 protests, internet traffic did not exceed 4-5% of normal figures for an entire week.[61] There is an extensive list of materials[62] prohibited for dissemination in Iran, including those calling for illegal actions, defaming the image of holy figures revered in Islam, and obstructing parliamentary elections. All state institutions are connected to a "special Internet" that is not accessible to those outside the country.

In the international arena, Iran sticks to an uncompromising anti-Western stance, but the country's influence on decision-making within key international institutions appears limited. Iran is active at the bilateral level in digital cooperation. Several digital security agreements are in place with Iran, including with Russia and China. Shared membership in the Shanghai Cooperation Organization, and now in BRICS, contributes to strengthening ties between these nations.

The Kingdom of Saudi Arabia (KSA) and the United Arab Emirates (UAE) are not only geographical neighbors, but also close partners in digital development. Both states, possessing significant hydrocarbon reserves, have achieved the highest levels of digital infrastructure and

[54] See the Concept of the Russian Federation on the organization, under the aegis of the UN, of a regular institutional dialogue involving all UN member states on security issues in the sphere of using ICTs as well as information and communication technologies per se // UN. URL: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/RUS_Regular_institutional__dialogue_Proposal_of_the_Russian_Federation.pdf

[55] See: Wunsch-Vincent S. WTO, E-commerce, and Information Technologies // Markle Foundation.
URL: https://metacept.com/wp-content/uploads/2019/10/Chapter-1.1.pdf

[56] African Bodies: AU AI Working Group holds first session // DataGuidance.
URL: https://www.dataguidance.com/news/african-bodies-au-ai-working-groupholds-first-session

[57] Iran // ITU Data Hub. URL: https://datahub.itu.int/data/?e=IRN

[58] Iran ICT Market Size & Share Analysis — Growth Trends & Forecasts (2024–2029) // Mordor Intelligence.
URL: https://www.mordorintelligence.com/industry-reports/iran-ict-market

[59] Some Critical Data Breach Statistics and Facts for People to Be Well Prepared To Fight Against Cybercrime // Enterprise Apps Today. 05.03.2024.
URL: https://www.enterpriseappstoday.com/stats/data-breach-statistics.html

[60] For example, see: the Competition Law: Islamic Republic of Iran "Law on Implementation of General Policies of Principle (44) of the constitution" // FAS of Russia. URL: https://fas.gov.ru/upload/other/ISLAMIC%20REPUBLIC%20OF%20IRAN%20LAW.pptx; Due to limited internet access within the country for users outside Iran, information on the Data Protection Law can only be obtained from indirect sources. See: Iran. Summary // DataProtection.
URL: https://www.dataguidance.com/jurisdiction/iran

[61] Internet disrupted in Iran amid fuel protests in multiple cities // NetBlocks. 15.11.2019.
URL: https://netblocks.org/reports/internet-disrupted-in-iran-amid-fuel-protests-in-multiple-cities-pA25L18b

[62] Hashemzadegan A., Gholami A. Internet Censorship in Iran: An Inside Look. Journal of Cyberspace Studies. 2022. Vol. 6(2). P. 183-204.

digital service accessibility for their populations. They boast that 100% of their residents use the Internet and 100% of the population are covered by fifth generation communication networks.[63]

The success in digitalization is not only due to the high level of wealth generated by oil exports, but also to the compactness of the population with its relatively small size, which is particularly evident with the UAE, where most of the country's 10 million residents live in the two largest emirates of Abu Dhabi and Dubai. Virtually the entire population of KSA and the UAE are active users of social networks, and the amount of data transferred per user a year is many times higher than the global average.[64]

Saudi Arabia and the UAE have established a common regime for regulating the circulation of user data, which has been in force in the two countries since 2023 and is based on the provisions of a special Data Protection Law.[65] Experts believe that it is based on the European GDPR.[66] While sharing the key definitions and concepts of the European model, the law in force in the KSA and the UAE differs, dictated by the cultural peculiarities of the two states. For example, according to the GDPR, a child is a person under the age of 16, while in the KSA and the UAE, this threshold has been reduced to 13. Cross-border data transfers are by default only to trusted jurisdictions and are not allowed without proper authorization from the competent authorities. Provisions for user data localization are in place.

Common to the two countries are the main characteristics of the digital market. International foreign digital platforms have a strong presence in these countries, leading the way in social media, messengers, and shopping sites. However, local companies compete successfully with foreign companies in food delivery, transportation, and tourist accommodation. The KSA and the UAE do not have specific laws in place to regulate digital market players for countering the threat of monopolization, but the level of market concentration in both countries is overall assessed as low.[67]

The rapid development of the digital economy in the KSA and the UAE has been associated with an increase in digital vulnerabilities, but assessments by the International Telecommunication Union suggest that the policies implemented in these countries are effective mainly in countering cyber threats.[68] Many ICT-related offenses are criminalized, punishable by up to 10 years in prison and fines of over USD 1 million. A common "weakness" of cybersecurity policies in these states is the lack of qualified personnel, which is identified as one of the main challenges in the respective strategic documents.[69] The KSA and the UAE are implementing policies to attract foreign specialists, as well as introducing requirements to develop the necessary competencies in educational programs.

The KSA is more active in the international arena, although the overall approach of Saudi Arabia and the UAE can be characterized as cautious and measured. The KSA enjoys its position as a member of the G20, but its current focus in the G20 is mainly on issues of a just energy transition, with digital development issues taking a back seat. The KSA and the UAE are reluctant to take on new international commitments and often join already announced initiatives that a stable circle of supporting countries already formed. For example, KSA representatives participated in UN OEWG meetings in 2019-2021, but never announced their own initiatives. Both states supported the recently submitted draft text of the WTO E-Commerce Regulatory Agreement (E-Commerce Joint Initiative).[70] A total of 80 WTO Member States have expressed support for this initiative.

[63] For example, see: Saudi Arabia // ITU Data Hub. URL: https://datahub.itu.int/data/?e=SAU; United Arab Emirates // ITU Data Hub. URL: https://datahub.itu.int/data/?e=ARE

[64] The world's average is 134 GB (see Note 45).

[65] Personal Data Protection Law // Saudi Data & AI Authority. URL: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf

[66] Sanjana S., Keyhani N. How does the new UAE Federal Decree Law on Personal Data Protection compare against the GDPR? // Bird & Bird. URL: https://www.twobirds.com/en/insights/2021/uae/how-does-the-new-uae-federal-decree-law-on-personal-data-protection-compare-against-the-gdpr

[67] Saudi Arabia ecommerce Market Size (2024–2029) // Mordor Intelligence. URL: https://www.mordorintelligence.com/industry-reports/saudi-arabia-ecommerce-market/market-size

[68] See: ITU Global Cybersecurity Index, 2020 // ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-R.pdf

[69] See: (Saudi Arabia) National Cybersecurity Strategy // National Competitiveness Center. URL: https://www.ncc.gov.sa/en/Aboutus/Pages/Cybersecurity.aspx; (UAE) National Cybersecurity Strategy // The United Arab Emirates' Government Portal. URL: https://u.ae/en/about-the-uae/strategies-initiativesand-awards/strategies-plans-and-visions/strategies-plans-and-visions-untill-2021/national-cybersecurity-strategy-2019

[70] Singh M. Saudi Arabia joins global e-commerce agreement // Gulf Business. 29.07.2024. URL: https://gulfbusiness.com/saudi-arabia-global-e-commerce-agreement

Conclusion

BRICS enlargement informally brings very different nations together in respect to digital policy. Undoubtedly, this is in keeping with the spirit of BRICS and its focus on representing the interests of the global majority in all its diversity. However, one cannot ignore the likely impact of the said differences on negotiation processes.

Digital security remains the most promising area of multilateral cooperation for the enlarged BRICS in the digital sphere. Four of the five new member states (Iran, Egypt, UAE, Saudi Arabia) share, at the conceptual level, the rigid approach of BRICS leaders — Russia and China — to realizing digital sovereignty. This fact, as well as the (partly) cross-membership of Russia, China, Iran, and India in the SCO, will allow for greater philosophical consolidation within the organization on issues of international information security and create prerequisites for more active practical cooperation, for example, in excluding undesirable narratives from the digital space and sharing information on cyber incidents that have occurred or are predicted to occur on terms of trust. Ideological convergence will make it possible to more effectively promote shared interests and values within key global institutions, especially the UN platform.

It is crucial to ensure that trust between BRICS member states is maintained and increased, especially amid persistent bilateral tensions. Not so long ago, Saudi Arabia and Iran did not have full diplomatic relations, while Egypt and Ethiopia have not yet reached a compromise on the use of water resources available in their region. BRICS must also retain its global, inter-civilizational character, avoid the problems characteristic of institutions supported by the countries of the global North, and avoid shifting the focus of the association's work predominantly to the problems of one region in light of the significant increase in the representation of African and Middle Eastern states.

The need for the development of digital infrastructure and human resources in the new BRICS member countries creates a demand for investment, qualified personnel and the exchange of best practices. Against this background, the revitalization of internal mechanisms of BRICS multilateral cooperation can be expected, as well as the formation of new initiatives and projects. In this process, it is important to keep a balance between the desire to create new platforms or mechanisms and the accompanying growth of intra-system pressures in order to maintain the achieved quality of multilateral cooperation within the association.[71]

On some issues, the inclusion of new members in the BRICS alliance means that new objectives need to be set. For example, it is crucial and desirable to consolidate the positions of BRICS members on e-commerce regulation and to start the process of harmonizing common approaches to protecting competition in digital markets. This can be effectively facilitated by joint multilateral consultations on an ongoing basis, as well as by creating a pool of best regulatory practices that have emerged in the BRICS space.

[71] Previous alarming trends in BRICS development. See: Ignatov A.A. BRICS Summit in Johannesburg: More Mechanisms and Less Concrete Decisions // Bulletin of the Peoples' Friendship University of Russia. Series: International Relations. 2019. Vol. 19. No. 1. P. 89-99.

Notes

Notes

РСМД

Российский совет
по международным
делам

Tel.: +7 (495) 225 6283
Fax: +7 (495) 225 6284
welcome@russiancouncil.ru

119049, Moscow,
8, 4th Dobryninsky pereulok

russiancouncil.ru