

https://dspace.org/

Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation

Belli, Luca

2021-12-06
LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://hdl.handle.net/10539/32208
Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. The African Journal of Information and Communication (AJIC), 28, 1-14. https://doi.org/10.23962/10539/32208

Downloaded from a DSpace repository. https://dspace.org/

Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation

Luca Belli
Professor of Internet Governance and Regulation, Head of Center for Technology and Society (CTS), and Head of CyberBRICS project, Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro
https://orcid.org/0000-0002-9997-2998

Abstract
In the concluding statement of the 2021 BRICS Summit, the bloc's five members—Brazil, Russia, India, China, and South Africa—pledged to pursue enhanced cooperation on cybersecurity issues, including by "establishing legal frameworks of cooperation among BRICS" and a BRICS intergovernmental agreement on cybersecurity. This piece briefly outlines the mounting relevance of cybersecurity for the BRICS countries, recent national policymaking in this area in the bloc, and the dynamics at play as the BRICS countries seek to further intensify and structure their cooperation on cybersecurity matters.

Keywords
cybersecurity, data protection, personal information, content moderation, cybercrime, policy, policymaking, BRICS, Brazil, Russia, India, China, South Africa

Acknowledgement
This piece draws on the contents of a blog post (Belli, 2021c) for the Directions blog of the European Union Institute for Security Studies (EUISS) Cyber Diplomacy Initiative (EU Cyber Direct). The author thanks Dr. Patryk Pawlak for feedback on the content of that blog.

DOI: https://doi.org/10.23962/10539/32208

Recommended citation
Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication (AJIC), 28*, 1-14.
https://doi.org/10.23962/10539/32208



This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:
https://creativecommons.org/licenses/by/4.0

1. Introduction

The 13th BRICS Summit, hosted by India on 9 September 2021, gave prominent attention to cybersecurity as one of the priorities identified in the Summit's concluding New Delhi Declaration (BRICS, 2021). Engagement and initiatives regarding cybersecurity by the BRICS countries—Brazil, Russia, India, China, and South Africa—have gained remarkable relevance in recent years. BRICS governments have adopted numerous laws that either explicitly frame cybersecurity or regulate some closely related aspects, and some of these legislative and regulatory initiatives may have a significant impact at the international level (see Belli, 2021a, 2021b). Importantly, the five countries' national approaches present several points of overlap and tend towards convergence, but at the same time we can identify significant points of divergence.

Despite growing alignment in several aspects of their priorities and policies, it is useful to recall that the BRICS bloc is a particularly young and unusual initiative, encompassing enormously different countries. After being created as a mere acronym, signifying countries with remarkable economic growth forecast,[1] in 2001, the BRICs organised their first informal meeting, in 2006, on the margins of that year's UN General Assembly. The first BRICs heads of state meeting was held in 2009 and, in 2011, the full integration of South Africa transformed the acronym into a larger and stronger BRICS. In 2014, the bloc established the BRICS-led New Development Bank,[2] its most prominent achievement, and, over subsequent years, more than 100 high-level events, partnerships, and initiatives have been promoted by the bloc every year.[3] This year, 2021, marks its 15th anniversary.

The BRICS' desire to cooperate on cybersecurity policy can be traced back to its 2013 eThekwini Declaration and Action Plan at the closing of the BRICS Summit in Durban, South Africa, which, for the first time, stated the need "to contribute to and participate in a peaceful, secure, and open cyberspace" and called for the elaboration of "universally accepted norms, standards and practices" (BRICS, 2013).

We should note that it was not a coincidence that BRICS countries' interest in digital policy issues related to cybersecurity—such as data protection, critical infrastructure security, cybercrime, and cyber defence—started to gain an increasingly essential and strategic role for the group in 2013 (see Belli, 2021b). It was indeed in that year that former US National Security Agency (NSA) contractor Edward Snowden (currently still in exile in Russia) revealed the unprecedented scale and pervasiveness of the

1 The acronym was first coined, in 2001, by a Goldman Sachs economist (O'Neill, 2001).
2 See https://www.ndb.int
3 For overviews of the evolution of BRICS, see Stuenkel (2016, 2020).

American-led global surveillance schemes which included, inter alia, the wiretapping of the personal phone of Brazilian President Dilma Rousseff (MacAskill & Dance, 2013).

BRICS cooperation in this area has intensified ever since. Notably, in the 2015 Ufa Declaration, at the conclusion of the 7th BRICS Summit, hosted by Russia, leaders established a "Working Group of Experts of the BRICS States on security in the use of ICTs" with a mandate to, inter alia, "develop practical cooperation with each other in order to address common security challenges in the use of ICTs" (BRICS, 2015). Also in that year, the BRICS ICT ministers signed a Memorandum of Understanding on Cooperation in Science, Technology, and Innovation (see Zhao et al., 2018), with the aim of promoting cooperation in these fields. Several concrete outputs followed these developments (see Belli, 2021b), including the BRICS Digital Partnership, the BRICS Partnership on New Industrial Revolution (PartNIR), the Innovation BRICS Network (iBRICS Network), and the BRICS Institute of Future Networks—all of which contributed to the construction of an enhanced cooperation process (see Belli, 2020b), combining policy, technology, and research initiatives.

The initiatives mentioned in this introductory section illustrate that the BRICS countries have adopted a remarkably interesting and sophisticated approach to cooperation and regulation. While agreeing on shared principles and high-level objectives through the annual declarations, they have crafted a blend of normative and developmental approaches to shape the ways in which their cooperation and regulation should unfold. Such an approach is not immediately intelligible for an observer used to considering only the normative side of regulation. Indeed, cooperation and regulation, be they on cybersecurity or on any other matters, cannot be achieved merely through norm-making. From a developmental perspective, it is much more effective to invest in research and development, rather than simply relying on norms in order to regulate economy, society, and technology.

The consideration proposed above, of the need to distinguish between normative and developmental dimensions of regulation, is essential to understanding the complexity of BRICS, before beginning the analysis of the latest normative policy steps taken by the group members. The primary aim of this article is, indeed, to focus on the increasing rapprochement of normative cybersecurity policy priorities and regulatory strategies across the grouping, rather than focusing on the developmental aspects of the bloc's approach to regulation. In this spirit, the following section provides an overview of some of the key policy developments, allowing the reader to understand how cybersecurity-related policies may be converging or diverging in specific areas.

2. Brazil

In 2020, Brazil adopted a new Cybersecurity Strategy,[4] enacted a new Data Protection Law[5] (best-known as "LGPD", in its Portuguese acronym), and tabled a regulation for social media content in the form of the Internet Freedom, Responsibility, and Transparency Bill (frequently referred to as the "Fake News Bill").[6] In mid-2021, Brazil created a new Federal Cyber Incident Management Network for federal public administrations[7] and rapidly adopted—and abandoned—the Executive Order 1068/2021,[8] altering the intermediary liability framework established by the Brazilian Internet Rights Framework (Marco Civil da Internet).[9]

The implications of these policy steps are mixed. The new Federal Cyber Incident Management Network is widely seen as welcome, but the Cybersecurity Strategy has been criticised for lacking the definition of objectives, budget, responsibilities, and deadlines—all of which are indeed the central elements of any strategy. The LGPD, strongly inspired by the EU's General Data Protection Regulation (GDPR), entered into force in September 2020, and represents a major step forward by introducing obligations to integrate privacy and data security measures into products and services—so-called "data protection by design". However, considerable work still needs to be done in terms of implementation. For example, despite the LGPD's creation of a new Data Protection Agency, Brazil witnesses major data leakages with remarkable frequency. In January 2021, personal data from the entire Brazilian population was leaked (see Belli, 2020a), and, while considerable advancements have occurred, the

4 See Decree nº 10.222/2020: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

5 See unofficial English version of the Brazilian General Data Protection Law: https://cyberbrics.info/brazilian-general-data-protection-law-lgpd-unofficial-english-version/

6 See Bill nº 2.630/2020: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944

7 See Secretaria Geral da Presidência da República (2021, July 19). Presidente Bolsonaro cria a Rede Federal de Gestão de Incidentes Cibernéticos: https://www.gov.br/secretariageral/pt-br/noticias/2021/julho/presidente-bolsonaro-cria-a-rede-federal-de-gestao-de-incidentes-ciberneticos

8 See https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.068-de-6-de-setembro-de-2021-343277275?s=08

9 Law 12.965/2014, known as the Brazilian Civil Rights Framework for the Internet, or Marco Civil da Internet (MCI) in Portuguese, is the federal law that establishes the principles and rules that govern the use of the internet in Brazil. Despite being categorised as an ordinary law, the MCI has been considered as the "Internet Constitution" of Brazil, because it defines the foundational elements of internet governance and regulation in the country, building into the law a marked intention to protect fundamental rights and freedoms online. The MCI is considered a symbol of participatory democracy due to the online consultation process that led to its creation. The process leading to the elaboration of the draft MCI bill was initiated and orchestrated by the Center for Technology and Society at Fundação Getulio Vargas (CTS-FGV), in partnership with the Brazilian Ministry of Justice and the Brazilian Internet Steering Committee (see CGI.br, 2014). While the elaboration of the MCI was initiated under President Luiz Inácio Lula da Silva, the processes culminated with the sanction of President Dilma Rousseff who, in response to intelligence revelations by NSA contractor Edward Snowden, called for the implementation of strong guarantees of human rights on the internet.

country is still far from having a data protection culture—one where all stakeholders are aware of data-related challenges, understand the social value of data protection, and cooperate to protect personal information (Belli & Doneda, 2021).

The proposed social media regulation (the Fake News Bill) has been criticised for introducing traceability requirements that would weaken encryption and raise the thorny issue of user-identification requirements (Iunes & Macedo, 2021). Notably, the Bill has raised such a level of criticism that the Special Rapporteur on Freedom of Expression of the Organisation of American States sent an official communication to Brazil stating that the provisions proposed in the original version of the Bill were "highly problematic in light of the principles of the right to freedom of expression consonant with Brazil's obligations under the International Covenant on Civil and Political Rights (ICCPR) and the American Convention on Human Rights (ACHR)."[10]

Meanwhile, the Executive Order altering intermediary liability had a very short life. As soon as it was adopted, it was unanimously criticised for the fact that it was likely to unduly affect freedom of expression and business operations. The Order aimed to prohibit social networks from removing misinformation when the content is of a "political, ideological, scientific, artistic or religious nature", even if contrary to a platform's terms of service. The Brazilian Supreme Court duly suspended the Order in September 2021,[11] less than two weeks after its adoption by the Federal Government, on the grounds that it was unconstitutional.

3. Russia

Russia enacted its Internet Sovereignty Law in 2019 (see Shcherbovitch et al., 2019), and, in 2021, amended its Data Protection Law and its Law on Information, IT and Protection of Information (see Zanfir-Fortuna & Iminova, 2021). The Internet Sovereignty Law purportedly aims to protect the country from cyberattacks. Under certain circumstances, it allows the Federal Government to mandate the disconnection of the Russian segment of the internet, the "Runet", from the global internet. While the extent to which Russia can implement an "infrastructure-embedded control" (Daucé & Musiani, 2021) of this sort remains unclear, the aim is overtly to be able to cut off its internet from the rest of the world (Musiani et al., 2019).

The Russian sovereign internet provisions aim at reproducing China's course of action in the early 2000s with its "Great Firewall of China", which created a large

10 See Relatoria Especial para a Liberdade de Expressão da CIDH. CIDH/RELE/Art. 41/7-2020/65 (3 July 2020): http://www.oas.org/es/cidh/expresion/documentos_basicos/PORTCARTAONUCIDH-BRASILINTERNET2020.pdf

11 See Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6.991 (14 September 2021): https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=757262152&prcID=6253449

national intranet that was connected through only limited channels to the rest of the internet outside the country. However, when China decided to implement its plan, at the dawn of the 21st century, the internet was much less pervasive than it is today. The Chinese citizens of the early 2000s were not reliant on the open internet for their everyday lives. The Russians of the 2020s, in contrast, have grown accustomed to a relatively open internet, making the necessary financial resources, personnel, technology, and disruption caused by the disconnection of the Runet significantly more complicated and intensive, compared to the situation in early 2000s China (Daucé & Musiani, 2021).

Amendments to two other Russian laws—the Data Protection Law and the Information Law—entered into force in March 2021. The amendments to the former create new requirements for personal data sharing and new oversight attributions for Roskomnadzor, the Federal Media and Information Regulator. The Information Law amendments require social networks to monitor content and "restrict access immediately" for users sharing information about sensitive matters such as state secrets, terrorism, pornography, promoting violence or riots, or using obscene language. These latter requirements have drawn objections from the European Court of Human Rights—to which Russia is subject, as a member of the Council of Europe[12]—that, in June 2020, criticised the law for allowing the government to take down or block online content without requiring a court order (see Grover & Thomas, 2021).

4. India

The Indian government made headlines in 2021 with its new Information Technology Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 ("IT Rules"),[13] and the tabling of the latest version of its Personal Data Protection (PDP) Bill is expected very soon.

The IT Rules establish a wide range of requirements, the most controversial of which are its social media content takedown framework and content traceability mandate (Rule 4(2)). The content takedown provisions are seen as excessively broad, as they allow the government to issue orders to intermediaries, requesting them to take down information hosted by them, thus considerably increasing the government's capability to restrict freedom of expression online. In respect of the Rule 4(2) content-tracing provision, major social media networks (i.e., those with more than 5 million users) now have an obligation to enable the tracing of the originators of content on their platforms, i.e., the social media platforms are required to keep a metadata trail

12 See https://www.coe.int/en/web/about-us/our-member-states

13 See Press Information Bureau of the Government of India (2021, February 25). Government notifies Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1700749

of their users' communications in order to be able to respond to government requests to trace specific messages.

This latter provision—as with the similar traceability provisions in the aforementioned Brazilian Fake News Bill—has been criticised for its potential to jeopardise the use of end-to-end encryption to maintain anonymity (SFLC.IN, 2021). Both WhatsApp and its parent company, Facebook—now also known as Meta—have filed petitions in the High Court of Delhi challenging Rule 4(2), emphasising that the provision undermines user privacy. WhatsApp contends that such a system requires it to *de facto* store metadata of each message sent though its platform, enabling "a new form of mass surveillance" (SFLC.IN, 2021).

The PDP Bill, when enacted, will help provide legal certainty on a variety of issues that intersect with those discussed above. Importantly, India is the only BRICS country that has not yet adopted a data protection law, and its PDP Bill is very similar in many respects to the other BRICS countries' frameworks.[14] The Bill aims to establish a comprehensive framework for regulating personal data processing, and is structured in 14 chapters that, inter alia, provide definitions; establish detailed obligations of the "data fiduciaries", including data security obligations; clarify the grounds for processing personal data; define the rights of "data principal"; and create a new regulator, the Data Protection Authority of India.

The first version of the PDP Bill was proposed by the government in 2018 in the aftermath of the Puttaswamy case (see CIS, 2020), a landmark decision by the Supreme Court of India that created a new fundamental right to privacy in the country. The Bill has been altered (and broadened) substantially in the intervening years, including the addition of a contentious section 35, which ascribes to the government an ample right to exempt governmental agencies from the application of the PDP Bill. Such evolutions led one of its original drafters, retired Supreme Court judge Justice B. N. Srikrishna, to characterise one of the Bill's most recent versions as "a blank cheque to the state" (Sircar, 2020).

5. China

China has been extremely busy in 2021 in respect of data-related policies, with special attention being paid to the cybersecurity dimension of data processing. China seems to be one of the few places in the world where policymaking outpaces technology developments and where regulation is strictly enforced (*The Economist*, 2021). The Chinese policy emphasis on data matters reflects Beijing's clear understanding of the key strategic advantage brought by having sound data protection and data security

14 For a detailed comparative analysis of the personal data frameworks of the BRICS countries, see https://cyberbrics.info/data-protection-across-brics-countries

frameworks (Belli, 2019), and its consideration of (personal) data—of which China is the largest producer globally—as an increasingly essential and valuable asset.

China enacted its new Civil Code[15] in January 2021, creating new legal rights to privacy and the protection of personal information. In August 2021, the Chinese National People's Congress adopted the new Personal Information Protection Law[16] (PIPL), and the Cyberspace Administration of China has since released a draft Regulation on Automobile Data Security for comment.[17] The PIPL, which may be seen as a GDPR with Chinese characteristics, defines China's comprehensive data protection system, setting general rules that are then to be specified according to the needs of particular sectors. To start complementing the PIPL, in October 2021 China adopted its Ethical Specifications of Next-Generation Artificial Intelligence,[18] and opened a consultation on Draft Guidance on Security Assessments for Cross-Border Data Transfers.[19]

In June 2021, Beijing adopted its new Data Security Law (DSL),[20] which defines more stringent requirements for processing "important data", "core state data", and "sensitive data", and extends (to all automated data-processing) the requirement to comply with the Multi-Level Protection Scheme (MLPS)[21] mandated by the 2017 Cybersecurity Law.[22] The DSL extends data localisation obligations, which mandate the storage of data in servers located in the national territory, to the aforementioned "important data". Article 21 of the DSL prescribes that "[e]ach region and department, shall stipulate a regional, departmental, as well as relevant industrial and sectoral important data specified catalogue, according to the data categorization." Important data listed in such catalogues may encompass an enormous spectrum of data linked to economic development, national security, the public interest, individuals'

15 See http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf

16 See https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

17 See https://www.gov.cn/xinwen/2021-05/12/content_5606075.htm

18 See https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html

19 See https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/

20 See the unofficial English version of China's Data Security Law: http://www.cov.com/-/media/files/corporate/publications/file_repository/data-security-law-bilingual.pdf

21 The MLPS is a cybersecurity compliance scheme that applies to virtually all organisations in China. It was first introduced in 1994 and subsequently updated in 2019, in accordance with Article 21 of the Cybersecurity Law. The MLPS classifies systems based on the damage that a hypothetical vulnerability of the system may pose to China's cybersecurity. The scheme requires all network operators to ensure that their networks are protected against interference, damage, or unauthorised access. Under MLPS, all network operators are required to classify their infrastructure and application systems on a 1 to 5 scale, and fulfil protection obligations accordingly. Systems ranked at 3 or higher are considered higher-stake, and are subject to notably stricter obligations, including on data security. See https://www.protiviti.com/HK-en/insights/pov-multiple-level-protection-scheme

22 See http://lawinfochina.com/display.aspx?id=22826&lib=law

rights, and corporates' interests. Such important data are subject to special security requirements as well as international transfer restrictions.[23] While the latest Chinese policies have strengthened data localisation obligations, it is important to note that such requirements were already present in the country, via the 2017 Cybersecurity Law, and were probably inspired by Russia's data localisation provisions introduced in 2015 (Shcherbovich, 2021).

In 2020, China adopted the Provisions on the Governance of the Online Information Content Ecosystem,[24] which play a major role in regulating online content. The Provisions define which categories of content are considered illegal, what content producers are encouraged to develop and publish, and an obligation to prevent the production of "undesirable" types of content. Illegal content includes any message instigating criminal activities or violence or defaming others. Encouraged content includes that which fosters "core socialist values", the doctrine of the Communist Party, and "positive and wholesome" messages. Undesirable content includes sensationalist headlines, coarse and vulgar language, gossip, and content that fosters improper habits that might be emulated by minors. Also in 2020, China announced its willingness to launch a Global Data Security Initiative, but so far this initiative has not gained meaningful traction.

6. South Africa

South Africa has also undertaken significant policy updates in 2021 that are relevant to cybersecurity (see Mabunda, 2021). As in the rest of the world, the COVID-19 pandemic has obliged the South African population to increasingly rely on electronic communications, connected devices, and digital services. While this has boosted the much-acclaimed "Fourth Industrial Revolution",[25] it has also offered an ideal ground for the proliferation of cybercrimes, including data breaches, online fraud, and identity theft. In June 2021, President Cyril Ramaphosa signed the new Cybercrimes Act of South Africa into law,[26] thus bringing the country up to date with international best practices. The Act creates new crimes in respect of certain types of access and interception of data, certain uses of software and hardware tools, and certain acts of interference with data or computer programs.

23 Appendix A of the Draft Guidelines for Cross-Border Data Transfer Security Assessments provides a detailed list of "important data" in different sectors. For instance, in the military sector, "important data" encompass information on the name, quantity, source and agent of purchased components, software, materials, industrial control equipment test instruments, geographical location, construction plans, security planning, secrecy level, plant drawings, storage volume, reserves of military research, and production institutions. See https://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

24 See the unofficial English translation of the Provisions on the Governance of the Online Ecosystem: https://www.chinalawtranslate.com/en/internetgovernance/

25 See Presidency of the Republic of South Africa (2020). *Report of the Presidential Commission on the Fourth Industrial Revolution*: https://cyberbrics.info/report-of-the-presidential-commission-on-the-fourth-industrial-revolution

26 See https://cyberbrics.info/cybercrime-act-south-africa/

In July 2021, the one-year grace period for the country's Protection of Personal Information Act (POPIA)[27] ended, thus making the law fully enforceable after an eight-year gestation period. The law was formally approved in 2013, but its implementation was subsequently put on hold while a new Information Regulator was established and South Africans were prepared for compliance. The Information Regulator is the data protection authority established by POPIA. Although it held its first meeting at the end of 2016, only in 2021 did it become able to duly monitor the implementation of POPIA, at the end of the grace period. POPIA draws significant inspiration from the European data protection regimes, establishing data protection principles, data subject rights, and an ample range of obligations, including security measures that must be implemented when processing personal data (according to sections 20 and 21 of POPIA). There are several points of intersection between POPIA and the Cybercrimes Act, due the latter's criminalisation of conduct that "interferes with a computer data storage medium or a computer system."[28]

It is interesting to note that South Africa is a signatory to the Council of Europe's Budapest Convention on Cybercrime,[29] despite not being a member of the Council. Meanwhile Russia, which is a Council member, has never signed the Convention and has been actively promoting international efforts to create a cybercrime treaty within the UN.

7. Enhanced cooperation at the international level?

As seen above, some parallels can be seen at national level in BRICS countries with respect to certain approaches to cybersecurity matters. At the same time, the countries' calls for enhanced cooperation, within the bloc, on such issues are becoming increasingly explicit (Belli, 2019). Indeed, in the aforementioned 2021 New Delhi Declaration, BRICS leaders expressed the intention to

> […] advance practical intra-BRICS cooperation in this domain, including through the implementation of the BRICS Roadmap of Practical Cooperation on ensuring Security in the Use of ICTs and the activities of the BRICS Working Group on Security in the use of ICTs, and underscore[d] also the importance of establishing legal frameworks of cooperation among BRICS States on this matter and acknowledge[d] the work towards consideration and elaboration of proposals, including on a BRICS intergovernmental agreement on cooperation on ensuring security in the use of ICTs and on bilateral agreements among BRICS countries. (BRICS, 2021)

The ease with which enhanced BRICS cooperation on cybersecurity matters can occur remains unclear. Cybercrime is a highly sensitive issue, and national

27 See https://popia.co.za/

28 For an analysis of the intersections, see Snail (2021).

29 See https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime

policymakers' decisions regarding which acts constitute cybercrimes are highly subject to their domestic legal, political, cultural, and economic particularities.

While South Africa has signed the Budapest Convention and Brazil has declared its intention to do so,[30] China, India, and Russia have not—and these three have a clear preference to coordinate their cybercrime initiatives within the UN and, to some extent, within the Shanghai Cooperation Organisation (SCO).[31] Since 2011, the SCO has elaborated upon an International Code of Conduct for Information Security, which was updated in 2015, reaffirming that "policy authority for Internet-related public policy issues is the sovereign right of States" and including the pledge "[n]ot to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security".[32]

When speaking as a bloc, the BRICS countries have consistently emphasised that the UN is the most appropriate venue for international policy development on cybersecurity and cybercrime. Willingness to enhance cooperation on such topics within the UN was recently reiterated by BRICS National Security Advisors,[33] and some members of this grouping have explicitly expressed interest in working on a "pentalateral" agreement to create a comprehensive system for countering cyber-threats. The BRICS 2021 New Delhi Declaration saluted the consensus found in the July 2021 report of the UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.[34] Conspicuously, the GGE was composed of experts from a grouping of 25 countries that included all of the BRICS nations and was chaired by Brazilian diplomat Guilherme Patriota, who is Brazil's Consul-General in Mumbai.[35]

30 See Ministério das Relações Exteriores (2019, December 11). Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores--e-do-ministerio-da-justica-e-seguranca-publica

31 The Shanghai Cooperation Organisation (SCO), http://eng.sectsco.org, is an intergovernmental organisation aimed at political, economic, and security cooperation. It covers three-fifths of the Eurasian continent, 40% of the world population, and more than 20% of global GDP. The SCO is the successor of the "Shanghai Five" group, established in 1996 with the Treaty on Deepening Military Trust in Border Regions, in Shanghai, by the heads of states of China, Russia, Kazakhstan, Kyrgyzstan, and Tajikistan.

32 See https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t858323.shtml

33 See BRICS National Security Advisors (2020). The 10th Meeting of BRICS National Security Advisors: https://india.mid.ru/en/counter_terrorism/10th_meeting_of_brics_national_security_advisors

34 See https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf

35 See https://www.un.org/disarmament/group-of-governmental-experts/

Russia has been calling for the development of an internationally binding treaty on cybercrime at the UN level since the early 2010s.[36] In December 2018, the UN General Assembly approved a resolution,[37] sponsored by Russia and a group of aligned countries, establishing an "open-ended ad hoc intergovernmental committee of experts" to "elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" under the auspices of the UN. While Russian proposals for a cybersecurity treaty have failed to crystallise sufficient consensus over the past decade, the most recent developments suggest that the situation is rapidly evolving, and that this initiative needs to be monitored closely, as numerous countries may now find the idea of a cybersecurity treaty appealing. The first substantial meeting of the ad hoc intergovernmental committee is planned for January 2022.

References

Ballard, M. (2010, April 20). UN rejects international cybercrime treaty. *Computer Weekly*. https://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty

Belli, L. (2019, November 13). From BRICS to CyberBRICS: New cybersecurity cooperation. *China Today*. http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html

Belli, L. (2020a, February 3). The largest personal data leakage in Brazilian history. *Open Democracy*. https://www.opendemocracy.net/en/largest-personal-data-leakage-brazilian-history/

Belli, L. (2020b). Data protection in the BRICS countries: Enhanced cooperation and convergence towards legal interoperability. CyberBRICS. https://cyberbrics.info/data-protection-in-the-brics-countries-enhanced-cooperation-and-convergence-towards-legal-interoperability/

Belli, L. (Ed.) (2021a). *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

Belli, L. (2021b). CyberBRICS: A multidimensional approach to cybersecurity for the BRICS. In L. Belli (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

Belli, L. (2021c, September 17). Cybersecurity convergence in the BRICS countries. [Blog post.] *Directions*. European Union. https://directionsblog.eu/cybersecurity-convergence-in-the-brics-countries/

Belli, L., & Doneda, D. (2021, September 2). O que falta ao Brasil e à América Latina para uma proteção de dados efetiva? JOTA. https://www.jota.info/opiniao-e-analise/artigos/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva-02092021

BRICS. (2013). eThekwini Declaration and Action Plan. http://mea.gov.in/bilateral-documents.htm?dtl/21482

36 See Ballard (2010).

37 See UN Doc. A/C.3/74/L.11/Rev.1: https://undocs.org/A/C.3/74/L.11/Rev.1

BRICS. (2015). VII BRICS Summit - Ufa Declaration. https://www.brics2021.gov.in/BRICSDocuments/2015/Ufa-Declaration-2015.pdf

BRICS. (2021). BRICS India 2021 - XIII BRICS Summit - New Delhi Declaration. https://brics2021.gov.in/brics/public/uploads/docpdf/getdocu-51.pdf

Centre for Internet and Society (CIS). (2020). The Centre for Internet and Society's comments and recommendations to the: The Personal Data Protection Bill 2019. https://cis-india.org/accessibility/blog/cis-comments-pdp-bill-2019

Comitê Gestor da Internet no Brasil (CGI.br). (2014, April 20). Um pouco sobre o Marco Civil da Internet. https://www.cgi.br/noticia/notas/um-pouco-sobre-o-marco-civil-da-internet

Daucé, F., & Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11685

Grover, G., & Thomas, A. (2021, February 22). Notes from a foreign field: The European Court of Human Rights on Russia's website blocking. CyberBRICS. https://cyberbrics.info/notes-from-a-foreign-field-the-european-court-of-human-rights-on-russias-website-blocking/

Iunes, J., & Macedo, N. (2021, June 1). Por onde anda o PL das Fake News? É necessário focar no aprimoramento dos deveres procedimentais, respeitando o regime de responsabilização adotado pelo Marco Civil da Internet. Portal FGV. https://portal.fgv.br/artigos/onde-anda-pl-fake-news-e-necessario-focar-aprimoramento-deveres-procedimentais-respeitando

Mabunda, S. (2021). Cybersecurity in South Africa: Towards best practices. In L. Belli (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

MacAskill, E., & Dance, G. (2013, November 1). NSA files: Decoded. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Musiani, F., Loveluck, B., Daucé, F., & Ermoshina, K. (2019, October 28). "Digital sovereignty": Can Russia cut off its internet from the rest of the world? *The Conversation*. https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952

O'Neill, J. (2001). *Building better global economic BRICs*. Global Economics Paper No. 66. Goldman Sachs. https://www.goldmansachs.com/insights/archive/archive-pdfs/build-better-brics.pdf

Shcherbovich, A. (2021). Data protection and cybersecurity legislation of the Russian Federation in the context of the "sovereignization" of the internet in Russia. In L. Belli (Ed.), *CyberBRICS: Cybersecurity regulations in the BRICS countries*. Springer.

Shcherbovitch, S., Granberg, S., & Carvalho, A. (2019, May 8). Sovereign internet law signed by the President of Russia. CyberBRICS. https://cyberbrics.info/sovereign-internet-law-signed-by-the-president-of-russia/

Sircar, S. (2020, March 3). A blank cheque to Govt: Justice Srikrishna on Data Protection Bill. *The Quint*. https://www.thequint.com/news/india/personal-data-protection-bill-a-blank-signed-cheque-to-government-justice-srikrishna

Snail, S. (2021, June 15). Legal intersections between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cyber Crimes Act 19 of 2020. CyberBRICS. https://cyberbrics.info/legal-intersections-between-the-protection-of-personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/

Software Freedom Law Center, India (SFLC.IN). (2021, May 28). Legal challenges to the traceability provision: What is happening in India? https://sflc.in/legal-challenges-traceability-provision-what-happening-india

Stuenkel, O. (2016). *Post-Western world: How emerging powers are remaking global order*. Polity Press.

Stuenkel, O. (2020). *The BRICS and the future of global order* (2nd ed.). Lexington Books.

The Economist. (2021, September 11). China has become a laboratory for the regulation of digital technology. https://www.economist.com/china/2021/09/11/china-has-become-a-laboratory-for-the-regulation-of-digital-technology

Zanfir-Fortuna, G., & Iminova, R. (2021, March 2). Russia: New law requires express consent for making personal data available to the public and for any subsequent dissemination. CyberBRICS. https://cyberbrics.info/russia-new-law-requires-express-consent-for-making-personal-data-available-to-the-public-and-for-any-subsequent-dissemination

Zhao, X., Li, M., Huang, M., & Sokolov, A. (Eds.). (2018). *BRICS innovative competitiveness report 2017*. https://publications.hse.ru/mirror/pubs/share/direct/252594344