CyberBRICS: Mapping Cybersecuity Frameworks in the BRICS

Luca Belli
Editor

Prefaces by *Sergio Suchodolski* and *Shen Yi*

PRE-LAUNCH BROCHURE

Please, quote this pre-launch brochure as:
Belli L. (Ed.) (Forthcoming) CyberBRICS: Mapping Cybersecuity Frameworks in the BRICS.

The opinions expressed in this volume are the sole responsibility of the authors and do not represent the position of the institutions that support this publication.

Edition produced by FGV Direito Rio
Praia de Botafogo, 190 | 13th floor
Rio de Janeiro | RJ | Brasil | Zip code: 22250-900
55 (21) 3799-5445
www.fgv.br/direitorio

CyberBRICS: Mapping Cybersecuity Frameworks in the BRICS

Luca Belli
Editor

Prefaces by *Sergio Suchodolski* and *Shen Yi*

PRE-LAUNCH BROCHURE

Please, quote this pre-launch brochure as:
Belli L. (Ed.) (Forthcoming) CyberBRICS: Mapping Cybersecuity Frameworks in the BRICS.

EDITION FGV Direito Rio

Work Licensed in Creative Commons
Attribution – NonCommercial – NoDerivs

Printed in Brazil
Completion of the First Edition in October 2019

This material, its results and conclusions are the responsibility of the authors and do not represent, in any way, the institutional position of the Getulio Vargas Foundation / FGV Direito Rio.

Coordination: Rodrigo Vianna, Sérgio França e Thaís Mesquita

Book cover: Andreza Moreira – Tangente Design

Layout: Andreza Moreira – Tangente Design

Reviewer: Luca Belli

Cataloguing data prepared by the Mario Henrique Simonsen/FGV Library

CONTENTS

PREFACE

Building universally accepted norms, standards and practices

Sergio Suchodolski

Steam was the protagonist of the first industrial revolution in the late eighteenth century. A century later, oil, electricity, and assembly lines made mass production possible. In the 1970s, automation, computers and connected networks generated the third revolution. Today the digital and the real mix inseparably. We are aligning artificial intelligence, IoT (Internet of Things), blockchain, 5G technology and digital analytics to drive real-world actions. It is the synergy between technological innovations and high scalability that leads to cost savings and facilitates access to new consumers.

While expanding connectivity and the emergence of new information and communication technologies (ICTs) have created opportunities for individuals and businesses, they also present a number of challenges, particularly regarding personal data regulation and cybersecurity governance. The increase in the number of new internet users in the BRICS countries has been remarkable over the last decade. The projection for the coming years is that the regions with the highest user growth will be in Latin America, Africa and Asia. The next billion users will probably come from the BRICS, along with the innovation and data they will produce and the policy they will need. This growth is pointed as one of the main causes of concern about cybersecurity due to the process of adaptation and learning of the population and local institutions, that could be vulnerable to cyber threats such as cyber terrorism, espionage, information sharing security, incident management, and cyber-crimes of different natures, including economic.

In this context, the BRICS countries are increasing their cooperation in the fields of science and technology and promoting synergies in relation to digital policies. Attention to issues that specifically involve cybersecurity, sovereignty and global governance has been growing in the BRICS countries in recent years. These subjects, which had been treated marginally at the official BRICS summits, became prominent from 2013. It was during the 5th BRICS Summit (2013) in Durban, South Africa, that countries signed the eThekwini Declaration recognizing the urgency of cybersecurity:

> *"We recognize the critical positive role the Internet plays globally in promoting economic, social and cultural development. We believe it's important to contribute to and participate in a peaceful, secure, and open cyberspace and we emphasize that security in the use of Information and Communication Technologies (ICTs) through universally accepted norms, standards and practices is of paramount importance".*

Since then, the debate has intensified, enlarging the scope of cybersecurity through cooperation, capacity-building, research & development, criminalization and global governance. Under these circumstances, the BRICS member countries must especially join forces, as we are in an increasingly liquid world. This VUCA (volatility, uncertainty, complexity and ambiguity) world faces a new technological revolution and challenges such as increased protectionism, the danger of terrorism and cybersecurity issues.

It is important to understand that not only the technological evolution and the economic progress of the members of Brazil, Russia, India, China and South Africa, but also the security of the 3.2 billion people who live in the BRICS countries, whose lives are being radically transformed by the digital revolution, are at stake. Some cybersecurity experts often use the following expression: There are only three types of users: those who have been hacked, those who will be hacked, and those who are currently being hacked.

As such, the pillar based CyberBRICS project of mapping existing regulations, identifying best practices and developing policy suggestions related to personal data protection and cybersecurity governance in BRICS is extremely adherent to the common challenges of block member countries. In addition, it is a vector to leverage digital transformation in developing common or – at least

– compatible solutions. CyberBRICS plays a key role in providing answers to these challenges by providing valuable – and as yet non-existent – information about BRICS digital policies, based on rigorously collected evidence that can be used by researchers, regulators and companies.

This work, didactically structured in 5 dimensions – protection of personal data; consumer protection; cybercrime; protection of public order; and cyberdefense – is a turning point and a great legacy as a way of what the BRICS must follow in this 4.0 world! The first and biggest challenge facing cybersecurity is raising awareness. This study connects directly with this gap, it examines and conveys what the real problems are. One of the most famous hackers in history, Kevin Mitnick, now one of the most respected cybersecurity professionals, has already said that a company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and other encryption technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.

About the Authors

Luca Belli, PhD is Professor of Internet Governance and Regulation at Fundação Getulio Vargas (FGV) Law School, where I also head the CyberBRICS project, and Associated Researcher at the Centre de Droit Public Comparé of Université Paris 2 Panthéon-Assas. Luca is also Member of the Board of the Alliance for Affordable Internet (A4AI) and member of the Programming Committee of the Computers, Privacy and Data Protection Conferences (CPDP). Before joining FGV, Luca worked as an agent for the Council of Europe (CoE) Internet Governance Unit and served as a Network Neutrality Expert for the CoE. Over the past decade, he has coordinated several research projects dedicated to digital policy and Internet governance, producing research outputs in English, French, Italian, Portuguese and Spanish, amongst which "De la gouvernance à la régulation de l'Internet" (Berger-Levrault, 2016); the "Net Neutrality Compendium" (Springer, 2016); "Community Networks: the Internet by the People, for the People" and "Platform Regulations: How Platforms are Regulated and How They Regulate Us" (FGV, 2017); "The Community Network Manual" (FGV-ITU-ISOC, 2018) and "Governança e Regulações da Internet na América Latina" (FGV 2019). Luca has been consulted by various international organisations and national regulators, including the International Telecommunications Union, the Secretariat of the Internet Governance Forum, the Internet Society and the French Telecoms Regulators. His works have been *i.a.* quoted by the Organization of American States Report on Freedom of Expression and the Internet (2013); used by the CoE to elaborate the Recommendation of the Committee of Ministers on Network Neutrality (2016); featured in the French Telecoms Regulator (ARCEP) Report on the State of the Internet (2018), and published or quoted by various media outlets, including Le Monde, BBC, The Hill, China Today, O Globo, El Pais and La Stampa.

Sergio Gusmão Suchodolski is the President of the Development Bank of Minas Gerais (BDMG), Brazil. Previously he was Director General, Strategy and Partnerships at the New Development Bank, in Shanghai, China. He has has served as Chief of Staff at BNDES – the Brazilian Development Bank. Prior to that, Mr. Suchodolski was Vice President for Corporate Development at Arlon Capital Partners, a New York based Global Private Equity Firm focused in Food and Agriculture investments. He holds a Master's of Laws Degree (LL.M.) from Harvard Law School, a Diplome (M.A.) from the Institut d'Etudes Politiques de Paris – Sciences-Po (Major in International Trade) and an LL.B. from the University of Sao Paulo Law School. Formerly, Mr. Suchodolski also held the positions of Special Advisor and Chief Foreign Policy Advisor at the Secretariat of Strategic Affairs, under the Office of the President of Brazil.

Shen Yi, PhD is Associate Professor at the School of International Relations and Public Affairs, Fudan University. He earned his Ph.D. at Fudan University in 2005 and severed as a research fellow at Fudan's Department of International Politics. He is currently the Director of the Research Center for the Global Cyberspace Governance, the non-resident researcher at the China Cyberspace Studying Institute, and individual director of China Association of Cybersecurity. The main research of Professor Shen Yi focuses on cybersecurity, cyber diplomacy and the governance of global cyberspace. From 2008 to 2009, Professor Shen Yi was a post-doctoral research fellow in the School of Foreign Affairs at Georgetown University. In 2013, Professor Shen Yi published his book on the National Cybersecurity Strategy of U.S. He participated the Conference of Cybersecurity and Informatization, which was hosted by President Xi Jinping on Apr. 19th, 2016, as one of the ten key speakers.

Daniel Oppermann, PhD is a research coordinator at the NUPRI Research Centre for International Relations (University of São Paulo, USP), in 2019 was a research fellow at the FGV Law School CyberBRICS project, and is a postdoctoral researcher at the School of Command and General Staff of the Army (ECEME) in Rio de Janeiro. He is a researcher of the Pró-Defesa IV Program of the Brazilian Ministry of Defence and the public research foundation CAPES. His research is focused on different aspects of Internet governance and cybersecurity. In 2018, Daniel edited the book "Internet Governance in the Global South – History, Theory and Contemporary Debates", published at the University of São Paulo. Daniel studied Political Science at the Free University of Berlin and holds a PhD in International Relations from the University of Brasília (UnB). He was a researcher at the OPSA Research Centre for South American Politics at the State University of Rio de Janeiro (UERJ) and a postdoctoral researcher at the Institute of Economy of the Federal University of Rio de Janeiro (UFRJ). As Chair of the Program Committee of the Global Internet Governance Academic Network (GigaNet), he coordinated the annual GigaNet Symposia in Brazil (2015) and Mexico (2016). Daniel has lectured on Internet governance, cybersecurity, geopolitics and data protection at the Federal University of Rio de Janeiro, at the DiGI School on Internet Governance (San Andrés University Buenos Aires) and at FGV Law School.

Andrey A. Shcherbovich, PhD graduated from the National Research University Higher School of Economics, Faculty of Law (Department of International Law) in 2008. He completed his Postgraduate studies at the National Research University – Higher School of Economics (Moscow, Russia) Faculty of Law (Department of Constitutional and Municipal Law) in 2011. From 2008 to 2010, he was affiliated as a Project Coordinator to the Non-Governmental Organization 'Inter-regional Library Cooperation Centre', a working body of the UNESCO Information For All Programme. From 2011 onward, he has been Associate Professor at the National Research University Higher School of Economics, Faculty of Law (Department of Constitutional and Municipal Law). From February to July 2019 he was a CyberBRICS Research Fellow at the Getulio Vargas Foundation Law School, Rio de Janeiro, Brazil.

Anja Kovacs, PhD directs the Internet Democracy Project in Delhi, India. The Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond. Anja's research and advocacy currently focuses on questions regarding data governance, surveillance and cybersecurity, and regarding freedom of expression – including work on gender, bodies, surveillance, and dataveillance, and gender and online abuse. She has also conducted extensive research on the architecture of Internet governance. Anja has been a member of the of the Investment Committee of the Digital Defenders Partnership and of the Steering Committee of Best Bits, a global network of civil society members, and is currently a member of the Board of Governors of Veres One. She has worked as an international consultant on Internet issues, including for the Independent Commission on Multilateralism, the United Nations Development Programme Asia Pacific and the UN Special Rapporteur on Freedom of Expression, Mr. Frank La Rue, as well as having been a Fellow at the Centre for Internet and Society in Bangalore, India. She is currently also a CyberBRICS Fellow at the Fundação Getulio Vargas (FGV) in Rio de Janeiro, Brazil. Prior to focusing her work on the information society, Anja researched and consulted on a wide range of development-related issues. She has lectured at the University of East Anglia, Norwich, UK, and Ambedkar University, Delhi, India, as well as guest lectured at universities in India and Brazil, and has conducted extensive fieldwork throughout South Asia. She obtained her PhD in Development Studies from the University of East Anglia in the UK.

Min Jiang, PhD is Associate Professor of Communication at UNC Charlotte and the 2019 CyberBRICS China Fellow at FGV Law School in Rio de Janeiro, Brazil. She is a secretariat member of the annual international Chinese Internet Research Conference (CIRC) and Associate Editor at Sage journal Communication & The Public. Her research focuses on Chinese Internet technologies (search engine, social media, big data), politics (digital activism, online political satire, diplomacy), business (Chinese Internet giants, business ethics), and policies (real-name registration, privacy). She has co-edited 3 special journal issues and published over 30 journal articles and book chapters on the Chinese Internet, some of which have appeared in Journal of Communication, New Media & Society, Information, Communication & Society, International Journal of Communication, International Communication Gazette, and Policy & Internet. Media outlets including Reuters, Deutsche Welle, Foreign Policy, Financial Times, The New Scientist, The Chronicle of Higher Education, Al Jazeera English have interviewed her for her work. She was born and raised in China. Prior to pursuing her doctor's degree in the U.S., she had worked at China Central Television (CCTV) and Kill Bill I in her native country China. Dr Jiang received her bachelor's and master's degrees from Beijing Foreign Studies University and her PhD in Communication from Purdue University.

Sagwadi Mabunda is a PhD Candidate at the University of the Western Cape. Her Doctoral thesis investigates the legislative responses of Cybercrime by analysing and critiquing the South African Cybercrimes Bill. She is a prolific speaker who has presented papers in numerous conferences both in South Africa and internationally (Italy, Germany, Namibia and Botswana). She has published a number of papers on her research interests which include Cybercrime and economic crimes such as International Anti-Money Laundering Law and International Anti-Corruption Law. She has also successfully organised the first annual Economic Crime and Cybercrime Conference (ECCC) hosted at the University of the Western Cape in collaboration with the Journal of Anti-Corruption Law (JACL). She has appeared as a guest lecturer at the University of the Western Cape, Cape Town and FGV Law School in Rio de Janeiro, Brazil on topics on the relationship between law and cybersecurity. She is currently working at the South African Constitutional Court as a Law Researcher, firstly to retired Justice Edwin Cameron, then to the Chief Justice Mogoeng Mogeong, and currently to Acting Justice Margaret Victor. In 2018 at age 25, Sagwadi was honoured as one of the Mail & Guardian 200 Young South Africans.

1 CyberBRICS: A Multidimensional Approach to Cybersecurity for the BRICS

Luca Belli

This book stems from the CyberBRICS project[1], which is the first initiative to develop a comparative analysis of the digital policies developed by BRICS (Brazil, Russia, India, China and South Africa) countries. BRICS have been chosen as a focus not only because their digital policies are affecting more than 40% of the global population – *i.e.* roughly 3.2 billion individuals living in such countries – but also all the individuals and businesses willing to use technologies developed in the BRICS or trading digital goods and services with these countries.

Digital policies and institutions elaborated and implemented by the BRICS are particularly interesting considering that such countries are already home to almost 40% of existing Internet users[2], who are both the producers of large amounts of personal data, frequently referred to as "the new oil[3]", "the new currency of the digital world,"[4] and "the world's most valuable resource[5]," as well as the potential developers and consumers of the technologies that will shape the evolution of the digital world.

Given the complexity of digital policies in general and cybersecurity in particular – not to mention the specificities of BRICS countries – this work aims at laying the foundation on which more research on cybersecurity and digital policy in the BRICS can and will be developed. To this end, the mapping exercise that this volume aims at conducting is truly fundamental, as it aims at laying the grounds upon which future comparative studies on BRICS digital policies can build and develop. It is indeed astonishing that, despite the

[1] The project is hosted by Fundação Getulio Vargas (FGV) Law School and developed in partnership with the Higher School of Economics, in Moscow, Russia; the Centre for Internet and Society, New Delhi, India; the Fudan University, Shanghai, China; and the University of Cape Town, Cape Town, South Africa. For further information see <https://cyberbrics.info/>; <https://cyberbrics.info/>.

[2] See <http://www.internetlivestats.com/internet-users-by-country/>.

[3] The phrase was coined by the British mathematician Clive Humby, in 2006, and was subsequently made popular by the World Economic Forum 2011 report on personal data. See WEF (2011).

[4] See Kuneva (2009).

[5] See The Economist (2017).

relevance of BRICS countries in today's evolving geopolitics, the weight of their digital economies, and the influence of their digital policies, no comprehensive comparative study of the BRICS digital policies exists to date.

This work is of particular importance, not only for researchers, digital policymakers, Internet users[6] and businesses, but for the BRICS themselves, considering that these countries are facing a twofold "digital paradox[7]." The expansion and cost-reduction of connectivity allows governments and businesses to offer a wide range of services, more efficiently than ever before, creating incredible social and economic opportunities through digital technologies. Yet, at the same time, such technologies enable cyber threats, cybercrime and cyberattacks[8] that limit the benefits promised by digital technologies and create a wide range of negative externalities that must be addressed by sound policies and regulations.

Furthermore, while recognising that digital technologies bring both significant benefits but also serious threats, public bodies and businesses in the BRICS are only beginning to implement – and in some cases are still elaborating – their digitalisation and cybersecurity strategies. The fact that strategies, regulations and institutions aimed at framing digital technologies in the BRICS have been – and are being – developed only very recently, and their impact is so potentially wide, provides an incredible opportunity for novel research in an incredibly stimulating area.

In this spirit, this volume represents the first important effort to systematise and analyse BRICS digital policies. This seminal CyberBRICS publication will focus on cybersecurity, while future research will explore two areas that are intimately intertwined with cybersecurity and are essential for the evolution of BRICS countries: connectivity policies, and strategies for digitalisation

[6] The term Internet user is utilised in this in its double nature of prosumer i.e. both producer and consumer of digital products and services. See Belli (2017:98).

[7] This concept has gained particular relevance at the South African level, as highlighted by Sagwadi Mabunda's analysis in Chapter 10 of this volume. See also: Department of Telecommunications and Postal Services, South Africa. (2017).

[8] See for instance Vaidya (2015); Department of Telecommunications and Postal Services, South Africa. (2017); Gemalto (2018).

of public administrations. This first work will provide an initial mapping, necessary to understand the state of play of BRICS digital policies and compare them, thus laying the foundations on which BRICS can build the future of digital policy research. The main goal of this volume is, therefore, to provide an understanding of how cybersecurity is conceptualised and structured in the BRICS, mapping the normative frameworks that regulate the various dimensions of cybersecurity in the BRICS and the institutions that implement these normative frameworks.

1.1 From BRICS to CyberBRICS

When Goldman Sachs economist Jim O'Neill coined the expression BRICs[9] in 2001 – without the capital "S", as South Africa would join only at a later stage[10] – the acronym simply aimed at identifying Brazil, Russia, India and China in the context of an economic forecast. Yet, the BRICs, subsequently evolved into BRICS, seized the occasion to start debating how a "Post-western World"[11] might look like, established dedicated diplomatic channels, promoted increasing synergies and coordination through dedicated working groups and partnerships in a wide range of diverse fields, culminating their joint aspirations with the creation of a joint institution, the New Development Bank, as well as the BRICS Contingent Reserve Agreement (CRA) in 2014.

Almost a decade in the making, BRICS are no longer a mere acronym, but have become a reality with progressively more intense relationships, a shared institution, and a continuously expanding agenda. Brazil, Russia, India, China and South Africa together represent over 40% of the world population, being home to 3.2 billion individuals, while generating 23% of the global GDP and 18% of the global trade. In addition to the presidential meetings, arranged through an annual summit and the informal

[9] See O'Neill (2001).

[10] The inclusion of South Africa in the group can be largely explained by the existence of the India-Brazil-South Africa Dialogue Forum or IBSA Trilateral, established in June 2003, as a mechanism for permanent coordination between the countries. The creation of IBSA signalled the strong political will to establish a longstanding partnership, collaborating to "the construction of a new international architecture; bring their voice together on global issues; deepen their ties in various areas." See <http://www.ibsa-trilateral.org/background.html>.

[11] See Stuenkel (2016).

meeting in the margins of the G20, the rotating Presidency of the BRICS organises nearly 100 official meetings every year, including approximately 15 ministerial meetings and dozens of gatherings of senior officials, discussing a wide spectrum of issues well beyond the original economic cooperation, such as digital technologies, climate change, cultural cooperation, education and many more[12].

BRICS countries are increasing their cooperation[13] in the field of digital policy and, especially, cybersecurity, which are becoming global priorities. Indeed, while the expansion of connectivity and the rise of new information and communications technologies (ICTs) are generating opportunities for individuals and businesses, they also pose several challenges, with particular regard to cybersecurity governance in its various dimensions, which can be addressed through shared and efficient policies. Since the BRICS ministers for science, technology and innovation met for the first time in 2014, the BRICS have remarkably intensified discussions in their areas of common interest and have started defining cooperation and partnerships, while adopting a number of shared documents[14], including a the Memorandum of Understanding on Cooperation in Science, Technology and Innovation[15] to design the legal framework within which the various branches of their cooperation can develop and expand.

Since 2014, the discussion of digital matters amongst the five countries has acquired notable prominence, including the promotion of a BRICS Digital Partnership[16] in 2016, the dedication of the 2018 Declaration of the BRICS Presidential Summit to a Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution[17], and the elaboration of an Enabling Framework for the Innovation BRICS Network[18]. These efforts BRICS

[12] See Brazilian Presidency of the BRICS. (2019).

[13] See BRICS (14 August 2019).

[14] For an analysis of such documents and their impact see Kiselev & Nechaeva (2018).

[15] The BRICS Memorandum of Understanding on Cooperation in Science, Technology and Innovation was approved at the second BRICS Science, Technology and Innovation Ministerial Meeting, held in Brasília, on 18 March 2015. See BRICS (18 March 2015).

[16] See BRICS Working Group on ICT Cooperation. (11 November 2016).

[17] See BRICS (2018).

[18] See BRICS STIEP WG (May 2019).

leaders have explicitly emphasised "the importance of continuing BRICS scientific, technical, innovation and entrepreneurship cooperation,"[19] and have already established concrete initiatives in this sense, including the BRICS Partnership on New Industrial Revolution (PartNIR), the Innovation BRICS Network (iBRICS Network), and the BRICS Institute of Future Networks[20].

BRICS's willingness to cooperate has recently shifted to the realm of digital policies, norms and standards as highlighted by the Xiamen Declaration, issued after the 9th BRICS Summit in 2017, according to which the countries committed to jointly "advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet[21]." In this spirit and with the aim to foster research collaboration and promote synergy regarding technology and policy development, BRICS have recently adopted a new BRICS Science, Technology and Innovation Work Plan 2019-2022[22] and established a new BRICS Science, Technology and Innovation (STI) cooperation mechanism called BRICS STI Architecture, aimed at:

- improving the coordination and management of BRICS STI activities through the definition of an agile cooperation governance structure;
- organising the different actions of cooperation according to their level of priority;
- measuring, monitoring and evaluating STI activities and initiatives, in order to minimise their development risks, make them result-oriented and optimise their real impact on society; and
- ensuring wide and effective dissemination of information about BRICS STI activities amongst different stakeholders including policymakers, scientists, research organisations and a wider audience[23].

[19] See Itamaraty (27 June 2019).

[20] Idem.

[21] See BRICS (2017).

[22] See BRICS (October 2019).

[23] See BRICS (September 2019).

It should be noted that BRICS countries have been chosen not only for their size and increasing economic and geopolitical relevance but also because, over the next decade, Internet growth is expected to occur massively in these countries, particularly in India, China and Brazil[24]. Hence, the technology, policy and governance arrangements defined by BRICS are likely to impact not only the 3.2 billion people that inhabit such countries but also the individuals and businesses that will choose to utilise increasing popular applications and services, as well as connected devices and networking equipment developed within BRICS countries based on BRICS standards.

The joint development of the BRICS Institutes of Future Networks, the BRICS Technology Transfer Cooperation and an Enabling Framework for the Innovation BRICS Network[25] concretely signal the group's willingness to enhance technological cooperation with particular regard to digital matters. Furthermore, the creation of both the first BRICS Technology Transfer Centre and the first BRICS Institute of Future Networks in China, respectively in Kunming[26] and Shenzhen[27], denotes the strong Chinese interest, proactiveness and financial commitment to promote and strengthen BRICS technological cooperation.

These evolutions highlight the mounting relevance of[28] and reliance on digital technology and digital economy for the BRICS and the pressing need for structured analyses on how such countries are addressing the challenges of digitality.

1.2 Why Focus on Cybersecurity?

The reason why cybersecurity has been chosen as the first broad theme to be analysed by the CyberBRICS project is that this topic has become a general concern for literally everyone in BRICS as

[24] Three BRICS countries, i.e. China, India and Brazil are the most populated countries of the regions where internet growth is expected to be the most relevant. See Cisco (2017).

[25] See BRICS STIEP WG (May 2019)

[26] See Kunming (11 September 2019).

[27] The first Institute has been established in Shenzhen, China, in August 2019. See XinhuaNet. (2019).

[28] See for instance Banga and Jeet Singh (2019); BRICS Competition Centre (2019).

well as non-BRICS countries alike. All citizens, businesses, public administrations, education institutions, and decision-makers must address cybersecurity in its various dimensions before some major risks and threats become reality. To borrow a very suited metaphor, cybersecurity is like "turbocharged climate-change"[29]. It is an issue affecting everyone and everything, although few realise its importance, and even fewer have a plan to address its challenges. Most start developing cybersecurity plans only after major accidents, substantial losses or disruptions. Critically, exactly like climate change, the only way to address cybersecurity efficiently and effectively is through cooperation involving all affected stakeholders[30].

Cybersecurity was a largely ignored concept by the general public until former NSA contractor, Edward Snowden exposed the massive hacking and surveillance schemes by NSA and brought cybersecurity issues that were previously reserved to a niche of specialists to the mainstream. Over the past few years, a number of institutions have recognised, as pointed out by the United Nations General Assembly, cybersecurity "is an increasingly important theme in international policy concerned with the digital economy and other aspects of the Information Society" primarily due to the fact "[t]here has been a growing incidence of serious cybersecurity attacks, some of which have had significant impacts on individuals and public services[31]."

To date, cybersecurity still is not a universally defined notion and its various dimensions and implications are largely ignored by the general public. Worryingly, such situation exists despite frequent cyberattacks, publicly disclosed data breaches[32] – which,

[29] I thank my friend Henrique Paiva for sharing this metaphor during his presentation at the CyberBRICS event on 5G and New Digital Infrastructures in the BRICS, held at FGV Law School on 30 August 2019. See <https://cyberbrics.info/event-5g-and-new-digital-infrastructures-in-the-brics/>.

[30] Formal agreement on the necessity to adopt a multistakeholder model to properly address cybersecurity has already emerged since the World Summit on Information Society, culminating in the adoption of the Tunis Agenda, whose paragraph 39 states that UN members "reaffirm the necessity to further promote, develop and implement in cooperation with all stakeholders a global culture of cybersecurity, as outlined in UNGA Resolution 57/239 and other relevant regional frameworks." See Tunis Agenda for the Information Society (18 November 2005). WSIS-05/TUNIS/DOC/6(Rev. 1)-E. <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

[31] UNGA (2018:4).

[32] According to the cybersecurity analysis firm Gemalto, during the first six months of 2018, "almost 1 billion records were compromised" only considering the breach incident of Indian digital identify programme Aadhaar, including the leak of Indian citizen names, addresses and a wide range of other personally identified information. See for instance: Gemalto. (2018).

under some regulatory frameworks[33], are now mandatory – and the juridical disputes between national governments and large companies, for a variety of cybersecurity-related issues, spanning from the usage of encryption techniques[34], to transnational flows of personal data[35] or the security of 5G networking equipment[36].

As an important premise of this work, it must be clarified that the notion of cybersecurity is a very elastic[37] one and may lead to deeply different interpretations, depending on the context. Several authors have explored how different approaches to cybersecurity are constructed, highlighting the existence of complementary but frequently diverging perspectives and stressing that cybersecurity definitions often crystallise around specific issues, threats, activities and aspects[38]. The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) provides a useful and overarching definition of cybersecurity, which is noteworthy for being a rare example of consensual cybersecurity definition at the international level, stating that:

> "*Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines,*

[33] Article 33 of the General Data Protection Regulation that entered in force in the European Union in May 2018 determines that personal data breach incidents must be notified to the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it". This norm, by itself is at the origin of a much greater awareness of the number of breaches occurring on a daily basis. It has also directly inspired the drafters of the Brazilian General Data Protection Legislation that, in its Article 48 foresees – in a less constringent tone than the EU Regulation – that "data breach notifications must occur within a reasonable time, to be defined by the national authority."

[34] See for instance Ewing (2016); Kolomychenko (2018).

[35] See for instance, the reasoning of the Court of Justice of the European Union declaring that the EU Commission's US Safe Harbour Decision is invalid, stressing that "the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country." Case C-362/14. Maximillian Schrems v Data Protection Commissioner. Press Release No 117/15. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.

[36] See for instance Sevastopulo and Bond (2019).

[37] Since the World Summit on Information Society, cybersecurity has been considered as an overarching concept encompassing a wide range of items and practices, including information sharing of national and regional approaches, good practices and guidelines; development of warning and incident response capabilities; establishment of suitable technical standards and industry solutions; harmonization of national legal approaches and establishment of international legal coordination; definition of sound privacy, data and consumer protection systems; and promotion of cybersecurity capacity building. See ITU (2005).

[38] For a recent and well-structure overview, see Fichtner (2018), discussing four approaches to cybersecurity, based on: data protection, safeguards of financial interests, protection of public and political infrastructures, and control of information and communication flows. For an analysis of different conceptualizations of cybersecurity, see also Wolff (2016).

> *risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment[39]."*

The amplitude provided by the above definition explains the need to have a more focused approach to define the boundaries for the discussions developed in this book. In this regard, the book concentrates on national frameworks defined and implemented by BRICS public bodies and purposely avoids exploring business practices, technical tools and assurances, and a potentially infinite list of diverse topics.

In this context, this volume starts from the premise that **five key dimensions of cybersecurity** can be identified as fundamental pillars that will orient our analysis. Such policy and governance dimensions will be presented in the five dedicated chapters and, subsequently, mapped in five country reports. Notably, the focus of our analysis will move from micro to macro, starting from **data protection** and then shifting to **consumer protection**, **cybercrime**, **the preservation of public order** and **cyberdefense**. These five dimensions have been chosen as the core avenues of our methodology. The goal of this publication is, therefore, to explore, map and present them so that, based on this work, a comparative approach can be developed.

This first chapter will introduce the volume, delimiting the concepts and issue areas that will be used in the country analyses while trying to identify general trends across BRICS countries. This chapter will be followed by five country-specific analyses, where the cybersecurity dimensions of each BRICS country are presented

[39] See ITU-T (2009).

and subsequently analysed in detail, by five country reports providing valuable insight on the various elements composing the cybersecurity frameworks of the BRICS.

To understand the relevance of BRICS digital policies in general and of this work in particular, the following section will provide an introduction to briefly explore the five cybersecurity dimensions mentioned above. Such presentation is instrumental in understanding the methodology used in this book and to taking the first step necessary to realise that BRICS are rapidly transitioning into CyberBRICS.

1.2.1 Cybersecurity Dimensions

Cybersecurity is a major concern for BRICS countries and beyond. States and their interconnected infrastructures – more recently dubbed as "smart" – may be potential targets, especially in the case of critical infrastructures that can become vulnerable when interconnected[40]. Cyberattacks can also put companies – from micro-enterprises to major players – at high risk. Further individual users are constantly lured into new connected services and devices with very little knowledge of the risks they face by increasingly exposing their lives to data collection with no precautions against potentially harms spanning from the abusive collection and usage of their personal data to a wide range of cybercrimes and cyberattacks.

While our awareness, preparation and protection levels are still largely inadequate, in BRICS as well as non-BRICS countries alike, the cybersecurity dimensions we analyse in the volume are increasingly – though still insufficiently – appreciated by various stakeholders who seem to be demanding and driving change. As the chapters and country reports dedicated to each specific BRICS country will highlight in this volume, several elements within the cybersecurity dimensions we identified are converging, and BRICS

[40] As an instance, in June 2019, the United States were reportedly "stepping up digital incursions into Russia's electric power grid in a warning to President Vladimir V. Putin and a demonstration of how the Trump administration is using new authorities to deploy cybertools more aggressively." According to the New York Times, "current and former [US] government officials described the previously unreported deployment of American computer code inside Russia's grid" by he United States Cyber Command, the arm of the Pentagon that runs the military's offensive and defensive operations in the online world. See Sanger & Perlroth (2019).

countries are increasingly adopting similar solutions to cope with shared challenges. On the one hand, such tendency towards compatible digital polices is largely due to the fact that digital technologies are distributed and utilised globally and therefore present global challenges to which all countries, including BRICS, are called upon elaborating efficient responses. On the other hand, BRICS may end up elaborating very similar digital policy and governance mechanisms as they not only influence each other's in their elaboration phase[41], but they may utilise similar models as sources of inspiration, especially when they do not have an existing policy in place to regulate specific digital issues.

The convergence of BRICS digital policies is illustrated, for instance, by the national data protection frameworks in the BRICS countries, which are becoming increasingly compatible on many fronts. This phenomenon is not due to any existing BRICS binding agreement on the matter. On the contrary, since the Xiamen Declaration, BRICS countries have expressed their willingness to jointly enhance their cooperation towards the definition of shared data protection norms[42] and, at the same time, they have considered the most comprehensive data protection frameworks that already exist – notably, the European Union's General Data Protection Regulation (GDPR) and the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* best known as Convention 108 – as a reference to shape their own national frameworks. The consideration of the same source of reference and the simultaneous recognition of the importance of data protection frameworks are therefore producing an interesting harmonization process.

This section provides an overview of the cybersecurity dimensions analysed in the volume, the methodology utilised to identify key elements of such dimensions as well as of the main BRICS tendencies that can be identified. We hope this first step in BRICS digital policy analysis can kick-start a much wider, deeper and

[41] As an instance, BRICS countries jointly agreed during the 9th BRICS Summit, in 2017, to jointly advocate for data protection and, after the 2017 Xiamen Declaration, all BRICS adopted or updated their data protection regimes.

[42] See BRICS (2017).

articulated effort, shedding light on a wide range of digital policy issues which are essential for the evolution of digitality in the BRICS countries and beyond.

1.3 Data Protection

Although much has yet to be accomplished in terms of affordability and availability of Internet access in BRICS countries, the past decade has witnessed an incredible increase not only in fixed Internet access – in some cases, due to massive public investments in network infrastructure[43] – but also in mobile coverage. This tendency together with the simultaneous adoption of smartphones and creation of systems of connected devices – in the context of the so-called Internet of Things (IoT) – allows for ubiquitous and permanent data collection, bringing important benefits[44] but also relevant risks.

In fact, the growing adoption of and reliance on digital services and devices increases significantly the potential for data collection and processing. Particularly, China, India, Brazil and Russia are, together with the USA, the countries currently having the most smartphone users in the world[45]. On the one hand, these evolutions have enormously increased the opportunities for data collection and exposed the potential that data, notably personal data, have in order to generate knowledge and value. On the other hand, they have also revealed that personal data should be considered as a key strategic resource whereas the lack of strong data protection frameworks, including effective implementation, may allow for an ample range of misbehaviours, spanning from privacy violation to interference in national governance. In this perspective, the lack of protection and security obligations regarding the collection and

[43] In China, significant government-led and policy-promoted investment in infrastructure are commonly acknowledged amongst the main driving forces that propelled the remarkable Internet growth undertaken by the country. See e.g. Boston Consulting Group (2017). A deeper analysis into the BRICS frameworks related to Internet access will be undertaken by the CyberBRICS project starting from 2020.

[44] The benefits derived from the expansion of connectivity as well as the advancement of the IoT can span from increased access to education, information and knowledge to gains in productivity, improved citizen participation, but also smoother transportations, more reliable electricity and cleaner environments. See e.g. World Bank (2016) and ITU (2016).

[45] These BRICS countries are respectively first, second, fourth and fifth nation with most smartphone users in the world. See Statista (2019).

processing of personal data may have detrimental consequences not only for individuals but also for national economies, security and democracy.

Since the adoption of the Tunis Agenda for the Information Society, during the second phase of the World Summit on Information Society, UN member states have agreed that cybersecurity "culture requires national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data[46]".

Data protection has therefore turned into an essential policy priority for BRICS countries as it is the central element of cybersecurity policy allowing to effectively regulate the security of personal information. Information security is commonly referred to as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction[47]. The analysis of BRICS data protection frameworks has therefore been considered as the first essential step to understand the complete picture of cybersecurity in the BRICS. While it must be acknowledged that a complete study of data protection requires the consideration of its legal, economic, and sociological dimensions, the analysis developed in the various Cybersecurity Country Reports featured in this book will only focus on the regulatory aspects of data protection in the BRICS. This is an explicit choice aimed at narrowing the focus to a specific aspect that can be more easily mapped and, subsequently, compared.

Aware of the fundamental importance of data protection for their economies, security and even sovereignty, all BRICS countries have recently established or updated their data protection frameworks and legislation. Major recent changes include:

- The adoption of a new Brazilian General Data Protection Law and the final approval of the establishment of a new Data Protection Authority[48];

[46] See Tunis Agenda, paragraph 39.

[47] This definition was originally proposed by the National Institute of Standards and Technology. See NIST (2003).

[48] See Section 1 of the Brazilian Country Report, in Chapter 3.

- The update of the Russian Data Protection legislation including data localisation provisions[49];
- The recognition of privacy as a fundamental right by the Indian Supreme Court and the ongoing elaboration of a new Data Protection Bill[50];
- Introduction of a new right to the protection of personal data in the new General Provisions of the Civil Code as well as data protection and data localisation norms in the Chinese Cybersecurity Law, further specified by the Personal Information Security Specification[51];
- The creation of a Data Protection Regulator in South Africa and the upcoming enactment of the Protection of Personal Information Act[52].

The above-mentioned legislations present various similarities, such as for instance the shared set of data subject rights and data protection principles. This is primarily due to the fact all BRICS countries considered European data protection as a reference to shape their national frameworks, either because they are directly affected – such as Russia, as a member of the Council of Europe – or because regulation compatible with European standards is increasingly essential to facilitate the free flow of information in digital economy. However, BRICS data protection frameworks also present many differences among each other and when compared to the European framework. A clear example is the Chinese Personal Information Security Specification that stands out of the BRICS data protection frameworks for being a non-binding document[53]. Interestingly, while it could be criticised for its limited force, the Specification includes a very innovative "Privacy Policy Template" providing a concrete blueprint for companies to meet data protection standards, revealing a different cultural approach based on "guiding by example".

Despite its non-binding character, the Chinese approach is interesting as it strives to orient organizations' behaviours by

[49] See Section 1 of the Russian Country Report, in Chapter 5.

[50] See Section 1 of the Indian Country Report, in Chapter 6.

[51] See Section 1 of the Chinese Country Report, in Chapter 9.

[52] See Section 1 of the South African Country Report, in Chapter 11.

[53] See Min Jiang's analysis in Chapter 8.

providing a model rather than by repressing the disrespect of the rule. Furthermore, this approach should be considered in conjunction with the recent announcement that the Chinese government will create a new National "Internet + Monitoring" System also called "China's Corporate Social Credit System" to monitor how all companies comply with the law, and raise sanctions for those who fail to comply or work with partners involved with fraudulent activities[54].

This may be an option to be explored beyond BRICS countries, considering that terms of service and the business practices of a conspicuous number of digital businesses frequently disrespect protection provisions, despite their binding force[55]. An alternative regulatory approach offering concrete guidance on how to properly frame business self-regulation, including guidance for data security, may be very useful to facilitate business compliance and avoid problems due to ignorance of the regulatory framework or lack of comprehension of proper implementation. In this sense, the study of BRICS solutions may be useful for BRICS and non-BRICS countries alike.

The adoption of data protection frameworks by all BRICS countries illustrates the double-purpose of data protection regulations, which play an essential role in not only preserving individuals' capability to enjoy an ample spectrum of rights[56] – including privacy, self-determination, and freedom of expression – but also promoting juridical certainty for businesses. Both rationales underpin data protection frameworks in BRICS countries, but their relevance may vary depending on the legal tradition of the specific country. As such, the emergence of a data protection culture in the BRICS stems from these two different but complementary visions of data protection as a body of law rooted in, on the one hand, the protection of individuals' rights and, on the other hand, the definition of clear rules

[54] See European Union Chamber of Commerce in China (2019).

[55] This phenomenon is particularly evident as regard terms of service of digital platforms. See Belli and Venturini (2016).

[56] In the BRICS context this approach has been very vocally reasserted by the Supreme Court of India, in 2017, with the adoption of its landmark Puttaswamy Judgement, stating that "the Right to Privacy is an integral part of Right to Life and Personal Liberty guaranteed in Article 21 of the Constitution." See WP (C) 494 of 2012, Justice K.S Puttaswamy (Retd.) v. Union of India and Ors.

fostering legal certainty for businesses and facilitating cross border data-flows. Importantly, in both perspectives, data protection plays an essential role as the main body of legislation fostering data security, not only as a principle but also through a concrete set of obligations and correspondent data subject rights.

As noted by UNCTAD, data protection is the body of law that defines the technical and organisational security measures that are indispensable to protect individuals against accidental loss, destruction of data, and deliberate acts of misuse. It provides threefold protection for the interests of individual data subjects, the entity processing the personal data and society at large[57]. Indeed, the existence of adequate personal data protection is essential not only for the cybersecurity of individuals but also for fostering trustworthy businesses environments and, by extension, national economies where risks are prevented and mitigated and responses to accidents and attacks are immediately enacted.

1.3.1 Data Protection Methodology

Questions for data protection methodology are grouped into five sub-dimensions: Scope, Definitions, Rights, Obligations and Sanctions, and Actors. To facilitate a better understanding and comparison of BRICS data protection frameworks, we invite readers to carefully consult the list of questions that every data protection section of the Country Report explores.

Scope

1. What national laws (or other types of normative acts) regulate the collection and use of personal data?
2. Is the country a party of any international data protection agreement?
3. What data is regulated?
4. Are there any exemptions?
5. To whom do the laws apply?
6. Do the laws apply to foreign entities that do not have a physical presence in the country?

[57] See UNCTAD (2016).

7. Definitions

8. How are personal data defined?

9. Are there special categories of personal data (*e.g.* sensitive data)?

10. How are the data controller and the data processor/operator defined?

11. What are the data protection principles and how are they defined?

Rights

12. Is the data protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

13. What are the rights of the data subjects according to the law?

Obligations and Sanctions

14. What are the obligations of the controllers and processors/operators?

15. Is notification to a national regulator or registration required before processing data?

16. Does the law require a privacy impact assessment to process any category of personal data?

17. What conditions must be met to ensure that personal data are processed lawfully?

18. What are the conditions for the expression of consent?

19. If the law foresees special categories of data, what are the conditions to ensure the lawfulness of processing of such data?

20. What are the security requirements for collecting and processing personal data?

21. Is there a requirement to store (certain types of) personal data inside the jurisdiction?

22. What are the requirements for transferring data outside the national jurisdiction?

23. Are data transfer agreements foreseen by the law?

24. Does the relevant national regulator need to approve the data transfer agreements?

25. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

Actors

26. What actors are responsible for the implementation of the data protection law?

27. What is the administrative structure of actors responsible for the implementation of the data protection law (*e.g.* independent authority, executive agency, judiciary)?

28. What are the powers of the actors responsible for the implementation of the data protection law?

1.4 Consumer Protection

Frequent data breaches[58] stemming from an ample range of vulnerabilities as a result of widespread adoption of connected devices underline the need for data protection and consumer protection.

The rise of digital technologies in the BRICS and beyond has not only created entirely new markets and digital marketplaces, but has also substantially changed the ways in which consumers interact and transact with (digital) good producers and service providers. Digital innovation has transformed both the nature of goods, services and commerce as well as the relations between consumers and producers/providers. Such a transformation is taking place at an impressive rate. In China e-commerce represents already more than 35% of the country's retail sales and the country's "Made in China 2025" strategy is planning to develop 95% of connected devices by 2025[59]. Indian e-commerce companies such as Snapdeal and Flipcart are already estimated to receive more than 70% of their orders via mobile phones[60]. South African technology investor Naspers has invested billions in BRICS start-ups over the past decade, substantially contributing to the success of some BRICS "unicorns" such as the Chinese technology giant Tencent and the Brazilian fintech Nubank[61].

In a context of increasing adoption of digital goods and services, consumer law frameworks are going to be essential to determine

[58] See e.g. Gemalto (2018).

[59] In this sense, see Min Jiang Analysis in chapter 8.

[60] See Bond (2019).

[61] See <https://www.naspersreport2019.com/>.

the degrees of security that individuals can expect when purchasing and utilizing (digital) goods and services. Furthermore, one can argue that consumer law will be increasingly tested as e-commerce and the IoT evolve in a symbiotic fashion further reducing the distinction between a good producer and a service provider, as all "thing" increasingly collect and process data and may include the capability to provide services. For instance, smart home devices and appliances, besides acting as connected products automating domestic tasks, can also serve as portals to communication or e-commerce services (such as smart speakers and virtual assistants). The growing adoption of such devices raises the question of how to properly categorize the smart-home device supplier: a producer of connected objects or a supplier of digital services? This categorization may have relevant consequences in term of responsibility of the producer or provider, as it is evident in the Russian context, where free online services, they are used "at one's risk", as consumer protection applies only to services provided in exchange of a payment[62].

The rise of the IoT is also a particularly relevant phenomenon, justifying the inclusion of consumer law as an essential cybersecurity dimension to be analysed in this book. Indeed, the IoT is increasingly multiplying the number of connected devices and the points of access for connected services while fostering new opportunities for interconnectivity between products and services. While this scenario can create many advantages for producers and consumers, it is also a growing cause for concern as any connected device represents a potential vulnerability that could be exploited by malevolent actors[63].

Due to the number of already existing connected devices and their projected growth[64] in the context of the IoT, the risk for cyberattack has considerably increased, moving from the digital environment to the physical environment where an ample range of

[62] See Andrey Shcherbovich's analysis in Chapter 4.

[63] See Belli (2019).

[64] According to the consultancy Statista, the "total installed base of Internet of Things (IoT) connected devices is projected to amount to 75.44 billion worldwide by 2025, a fivefold increase in ten years." See <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.

poorly secured[65] – or sometimes completely unsecured – devices are utilised by many users largely uninformed about cybersecurity. This proliferation of connected and potentially hackable devices raises the question as to what the most appropriate regulatory tool could be to prevent, mitigate or, ideally, eliminate the risks of cyberattacks.

It is important to note that the increase of cyberattacks is not only due to the numerical growth of connected devices. Indeed, the expansion of the IoT must be considered together with the simultaneous lack of security systems incorporated in the design of the connected products or services combined with the lack of consumer awareness regarding cybersecurity risks. IoT security is a major challenge. Attacks exploiting connected devices can be relatively easy to implement primarily because security is not the main preoccupation of product developers and investing in security raises development costs. The proliferation of connected devices from things we can wear to things we have in our homes further contributes to the vulnerability of cyberattack.

A telling example is the Mirai Botnet, a malicious software behind a series of massive distributed denial of service (DDoS) attacks in October 2016. Mirai infected hundreds of thousands of insecure consumer IoT devices that utilised the most common factory default usernames and passwords[66]. Both government portals and popular commercial services (such as Amazon, Netflix, Spotify and Twitter) were significantly disturbed and Brazil was among the most hit countries, alongside China, Russia and India in the top ten of the most affected[67].

An important observation to be made is that awareness-raising and education are essential to consumer protection in particular and to all cybersecurity dimensions in general. Major capacity building and awareness-raising efforts need to be organised to target all audiences: consumers and internet users, especially children, teachers, researchers, governmental officials, and industrial actors.

[65] See Mosenia and Jha (2016).

[66] Marzano et al. (2018).

[67] See Antonakakis et al. (2017).

The Mirai example usefully illustrates the total unpreparedness of all stakeholders alike. Despite knowledge of the Mirai botnet, new variants keep on being discovered and attacks are mounting, primarily due to very poor security standards implemented by connected devices producers[68].

In this context, while personal data protection plays an essential role in preventing personal-data-related risks in the context of the IoT, the body of law that becomes essential to regulate the security of connected devices is consumer protection law. Both bodies of law are crucial, but user rights and consumer rights cannot be protected in the face of mounting risks if data subjects and consumers are not fully aware of their rights and risks involved or ways to mitigate such risks. As such, it is particularly relevant to map national consumer protection frameworks to have a clear understanding of what rights, obligations and security standards should consumers, producers and providers expect when choosing digital goods and services originating from the BRICS countries.

1.4.1 Consumer Protection Methodology

To facilitate the reader's comparison of the various consumer protection dimension, the same sub-dimensions utilised to map data protection frameworks were adopted, including the following five sets of questions tailored for consumer protection.

Scope

29. What national laws (or other types of normative acts) regulate consumer protection?

30. Is the country a party of any international consumer protection agreement?

31. To whom do consumer protection laws apply?

32. Do the laws apply to foreign entities that do not have a physical presence in the country?

Definitions

33. How is consumer protection defined?

[68] See Pankov (2019).

34. How are consumers defined?

35. How are providers and producers defined?

36. Does the law provide any specific definitions with regards to consumer protection in the digital sphere?

Rights

37. Is the consumer protection law based on fundamental rights (defined in Constitutional law or International binding documents)?

38. What are the rights of the consumer defined by the law with reference to digital goods and services?

39. Is consumer protection law applicable to users of zero price services, *i.e.* free of charge?

Obligations and Sanctions

40. Does the law establish specific security requirements to provide digital services or goods?

41. What are the sanctions and remedies foreseen by the law for not complying with the obligations?

Actors

42. What bodies are responsible for the implementation of the consumer protection law?

43. Is there a specific consumer protection body? If so, what is its administrative structure?

44. What are the powers of the bodies responsible for the implementation of the consumer protection law?

1.5 Cybercrime

Cybercrime law is the body of law that defines what acts perpetrated via or against ICT systems should be considered as illegal and what measures and procedures should be followed to investigate such acts. As such, cybercrime can be considered either as a component of cybersecurity or at least as a field that largely juxtaposes to cybersecurity. Assuming that the main concern of cybersecurity is to foster security within ICT systems, thus protecting users and assets from any potential threats, it becomes useful to identify what activities should be categorised as malicious use of ICT systems and how they could be investigated and repressed. In this sense, the fact that the UN General Assembly, in its 2010 Resolution on Cybersecurity[69] addresses cybercrime as a core dimension of cybersecurity stresses the general tendency to consider them intimately intertwined issues.

In this perspective, the works of the ITU (2009; 2014) highlight cybercrime as an essential component of cybersecurity, stressing the importance of addressing it in national cybersecurity strategies. ITU clearly suggests that UN members adopt dedicated legislation addressing behaviours that can be categorised as criminal use of ICTs[70]. On the other hand, the UN members have agreed upon the benefits of multi-stakeholder[71] cooperation with regard to cybercrime[72]. Indeed, cybersecurity strategies and cybercrime frameworks, although crafted by public bodies, generally start with the consideration that cybercrime prevention, response and recovery need to rely on multi-stakeholder coordination, including private sector and individual users of ICT as partners in the implementation – and frequently also the elaboration – of public policies.

Furthermore, as pointed out by the ITU (2014), a general assumption of any cybersecurity or cybercrime strategy is that cyber threats are rarely national and generally have a cross-border nature. This is because the various intermediaries involved in the operation of the services and digital tools utilised to perpetrate a crime are rarely located all in the same jurisdiction[73]. In this perspective, the emergence of a shared – or at least convergent and compatible – BRICS legal framework on cybersecurity in general and cybercrime in particular seems to be a shared priority for BRICS that are

[69] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[70] See ITU (2014).

[71] For an analysis of benefits as well as inconveniences determined by multistakeholder governance and models, see Belli (2015; 2016).

[72] Particularly, the Tunis Agenda, in its paragraph 40, affirms "the necessity of effective and efficient tools and actions, at national and international levels, to promote international cooperation among, inter alia, law-enforcement agencies on cybercrime [and] call[s] upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime."

[73] This situation has led Russia to enact "Internet Sovereignty" legislation, to reterritorialize digital environment, as illustrated by Andrey Shcherbovich analysis. See chapter 4 and the following Russian Country Report.

increasingly exploring options to enhance their cooperation via the dedicated BRICS Working Group on Security in the Use of ICTs[74].

However, despite being a central aspect of cybersecurity, cybercrime may be challenging to delineate in research due to the lack of an international agreement on what elements compose it. This is particularly true since, despite the transnational nature of cybercrime, the definition of what activities in particular shall be deemed as criminal fall within the quintessentially national remit.

It may be argued that "cybercrime" encompasses a wide range of activities outlawed in specific jurisdictions and committed either by using ICT systems as an enabler in order to commit the crime or targeting specific ICT systems and the data that they store[75]. The ITU Global Programme on Cybercrime[76] offers two useful taxonomies of the offences that may be considered as cybercrimes. We consider two taxonomies for cybercrime below.

The first taxonomy is broader and considers whether digital technology is necessary to perpetuate the offence or simply enables the offence. To this central distinction, the ITU Global Programme on Cybercrime adds a third category, specially dedicated to online child sexual exploitation and abuse, as follows:

i) Cyber-dependent crime: it requires an ICT infrastructure and involves the creation, dissemination and deployment of malware, ransomware, attacks on critical national infrastructure (e.g. the cyber-takeover of a power-plant by an organised crime group) and taking a website offline by overloading it with data (a DDOS attack).

ii) Cyber-enabled crime: it can occur in the offline world but can also be facilitated by ICT. This typically includes online frauds, purchases of drugs online and online money laundering.

iii) Child sexual exploitation and abuse: it includes abuse on the clear Internet, darknet forums and, increasingly, the exploitation of self-created imagery via extortion – known as "sextortion".

[74] Cybercrime and cyber-attacks are considered as transnational security issues to be maintained as "Main areas of cooperation" for BRICS countries. See <http://brics2019.itamaraty.gov.br/en/about-brics/main-areas-of-cooperation>.

[75] See World Bank (2017:66).

[76] See <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html>.

The second taxonomy is based on the instrumental relationship between digital means and the specific offences. This categorization draws from the Convention on Cybercrime of the Council of Europe[77], better known as the Budapest Convention, clustering offences in four categories:

i) Offences against the confidentiality, integrity and availability of computer data and systems;

ii) Computer-related offences;

iii) Content-related offences;

iv) Offences related to infringements of copyright and related rights.

As it emerges from the abovementioned taxonomies, the details of what can be considered cybercrime may – sometimes strongly – vary from country to country, especially when it comes to offences beyond the core of cybercrime. As pointed out by UNODC (2013), the core of cybercrime is composed of a limited number of acts against the confidentiality, integrity and availability of computer data or systems[78]. Beyond this core, whether a computer-related and computer content-related offence can be categorised as "cybercrime" is not universally agreed upon due to national juridical traditions and political sensitivities.

Given this context, the fact that BRICS countries have very different conceptions of cybercrime due to the different type and depth of the cybercrime debate in each country should not be a surprise. For instance, while in China the Criminal Law (1997) and Cybersecurity Law (2017) provide a very detailed list of what online behaviours shall be deemed as criminal[79], in Brazil only a few of the conducts that may be categorized as cybercrime are *de facto* penalized by law[80]. The Criminal law of Russia, in its general and special parts,

[77] The Convention on Cybercrime of the Council of Europe (CETS No.185) is the only binding international instrument specially dedicated to framing cybercrime issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between treaty signatories. Interestingly, South Africa is the only BRICS member to be a signatory of the Budapest Convention while Russia, which is a Council of Europe member, is not a signatory. See <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

[78] See UNODC (2013).

[79] See the Cybercrime section of the Chinese Country Report, in Chapter 9.

[80] See Daniel Oppermann's analysis in chapter 2 of this volume.

also offers a rather detailed overview of cybercrimes[81] and related sanctions while in South Africa, until the new Cybercrime Bill will enter in force, cybercriminal conducts remain primarily defined only in a sectorial fashion by the Electronic Communications and Transactions Act[82]. India interestingly adopts a hybrid approach, providing sometimes detailed definitions of the constituent elements of the cybercrimes listed by the IT (Amendment) Act but remaining rather vague on the definition of the cybercrimes themselves[83].

To offer a better understanding of what behaviours can be considered as cybercrime and how criminal law de facto influences cybersecurity policy development in the BRICS, the CyberBRICS project has adapted its penta-dimensional framework adding a further sub-dimension dedicated to procedural law.

1.5.1 Cybercrime Methodology

Scope

45. What national laws (or other types of normative acts) regulate cybercrime?

46. Is the country a party of any international cybercrime agreement?

47. What cybercrimes are regulated?

48. To whom do the laws apply?

49. Do the laws apply to foreign entities that do not have a physical presence in the country?

Definitions

50. How is cybercrime generally defined by the national law?

51. What are the cybercrimes provided for by the law and how are they defined?

52. How is a computer system defined?

53. How are computer data defined?

[81] See the Cybercrime section of the Russian Country Report, in Chapter 5.

[82] See Sagwadi Mabunda analysis in Chapter 10 and the cybercrime section of the South African Country Report I Chapter 11.

[83] See Anja Kovacs' Analysis in Chapter 5 and the Cybercrime section of the Indian Country Report, in Chapter 7.

54. How are forensic data defined?

55. How are service providers defined?

56. Does the national law provide any other definitions instrumental to the application of cybercrime legislation?

Rights

57. Is the cybercrime law based on fundamental rights (defined in Constitutional law or International binding documents)?

58. What are the rights of the victim and the accused?

Procedures

59. Is there a specific procedure to identify, analyse, relate, categorize, assess and establish causes associated with forensic data regarding cybercrimes?

60. In the case of transnational crimes, how is cooperation between the national law enforcement agency and the foreign agents regulated?

61. Is there any exception to the use of mutual legal assistance procedure to investigate the crime?

62. Does the national law require the use of measures to prevent cybercrimes? If so, what are they?

Obligations and Sanctions

63. What obligations do law enforcement agencies have to protect the data of the suspect, the accused and the victim?

64. What are the duties and obligations of the National Prosecuting Authorities in cases of cybercrime?

65. Does the law impose any obligations on services providers in connection with cybercrime?

66. To which extent can a legal person be held liable for actions in connection with cybercrimes?

Actors

67. What bodies implement the cybercrime legislation?

68. Is there a special public prosecutor office for cybercrime? If so, how is it organised?

69. Does the cybercrime legislation create any specific body?

1.6 Public Order

The preservation of public order – frequently referred to using the French expression "*ordre public"* – is considered, under international law, as a rightful justification for imposing limitations to fundamental rights and freedoms. According to the International Covenant on Civil and Political Rights, for instance, a number of fundamental rights, including the right to freedom of expression, the right of peaceful assembly, the right to freedom of association with others, and the liberty of movement, can be rightfully restricted by law, when such restrictions are "necessary to protect public order[84]." The contours of the notion, however, are particularly fuzzy and, for this reason, the preservation of public order must be pursued within specific rule of law frameworks delineating when it is appropriate to invoke public order as a legitimate justification and which authorities can implement police functions and under what circumstances.

While the term "police" generally refers to bodies whose fundamental purpose is to preserve public order and public safety through the enforcement of rules and assisting the public, the police function may acquire a different nature when applied to the digital environment as it is increasingly delegated to non-public actors[85]. In this case, the rule of law requirement becomes even fuzzier in the context of an increasing delegation of police functions to private Internet intermediaries[86].

The protection and preservation of public order and morality are at the core of administrative policing, the objectives of which are unique to every country. On the other hand, judicial policing has a repressive character, aimed at recording offences against criminal law, gathering evidence and searching for the perpetrators of specific offences[87]. To distinguish between administrative and

[84] See e.g. ICCPR (1966) art. 12, 19, 21 and 22. Importantly, the degree of "necessity" is generally evaluated considering the legitimacy of the goal established by law and the proportionality of the measures. In this perspective the UN Human Rights Council has consistently stated that "Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those, which might achieve the desired result; and they must be proportionate to the interest to be protected." See e.g. UNHRC General Comments No. 27/1999 and No. 34/2004.

[85] See Belli & Sappa (2017).

[86] See Belli, Francisco & Zingales (2017).

[87] Idem.

judicial policing, it is important to consider the intent for which police operations are undertaken. Particularly, it depends on the existence of a link between a police operation and a criminal offence: administrative policing is aimed at the general preservation of public order and morality; judicial policing is aimed at the special repression of given offences.

In this perspective, Internet intermediaries implementing specific content management measures – such as China's elaborate content management system[88] aimed at removing or disabling access to specific content in order to protect public order – act as administrative police. On the other hand, Internet intermediaries retaining personal data of (cyber)criminal offenders or blocking access to content in compliance with court decisions act as criminal police. As such, private intermediaries can act as cyber-police to monitor the implementation of national legislation.

To analyse the specific normative measures allowing for the preservation of public order as well as the existence of specific "cyber measures" involving private intermediaries in the implementation of national law, the methodology developed by the CyberBRICS project has included a specific dimension dedicated to public order.

1.6.1 Public Order Methodology

Definitions

70. How are public order, threats to public order and the protection of public order defined?

71. Is the protection of public order grounded in constitutional norms?

Measures

72. What cyber measures address threats to public order?

Actors

73. What public authorities are responsible for the implementation of surveillance techniques?

[88] See Min Jiang's analysis in Chapter 8 as well as the Chinese Country Report.

74. What are the obligations of these public authorities?

75. Can private actors be involved in the implementation of cyber measures to address threats to public order?

1.7 Cyberdefense

The last dimension considered by this volume is cyberdefense, which is essential to give force to the overall policy efforts and governance mechanisms aimed at improving each country's cybersecurity. Cyberdefense mechanisms and, particularly, the type measures necessary to handle cyberattacks and cyber threats are frequently developed and enacted as a reaction to disruptive events. This is the case for instance, of Brazil, where cyberdefense started to be a topic of interest in the aftermath of a series of web defacement attacks in 2011when a larger number of public service portals and government websites went offline for several hours[89].

This dimension typically falls under the purview of a country's national security policy, including operational actions deployed for offensive and counter-offensive combats in cyberspace. For this reason, cyberdefense is commonly linked to countries' military and intelligence services[90]. The country reports included in this book show that this tendency is also shared by BRICS countries, with a strong military presence.

Furthermore, a distinguishing trait of cyberdefense is that it is typically elaborated and implemented by the Executive. This means cyberdefense is usually shaped directly by the national defence ministry or administration and is closely intertwined with secret and classified aspects of government policy and activity[91]. This is particularly evident in the Russian case, where cyberdefense is primarily shaped by official doctrines defined by the President of the Russian Federation, acting in his constitutional role of Supreme Commander of the Armed Forces[92].

[89] See Daniel Oppermann's analysis in chapter 2 of this volume.

[90] See Canongia & Mandarino (2012).

[91] See Dewar (2018).

[92] The Military Doctrine of the Russian Federation and the Russian Doctrine of Information Security are particularly relevant in this regard, as pointed out by Andrey Shcherbovich's analysis in Chapter 4.

While the other cybersecurity dimensions are defined by policies typically released into the public domain, cyberdefense may have a non-public nature, due to its particular sensitivity. While some aspects of cyberdefense are public, such as what events shall be considered as a cyberattack, what are the criteria for attributability of the responsibility in cyberattacks and what measures will be taken as self-defence against such attacks, other elements may be much less clear and public such as to which extent cyber offence or interventions in other countries' systems or infrastructures are deemed as admissible and de facto undertaken. Therefore, it is important to acknowledge that, due to its highly sensitive nature, many elements of cyberdefense may be secret and this peculiarity makes it more challenging to have a complete picture and a clear understanding of the national frameworks.

It can be argued that cyberdefense strategies and frameworks primarily focus on two axes: on the one hand, the defensive measures that can improve robustness and resilience of national infrastructures and systems that are deemed as critical; on the other hand, the measures that can prevent and avoid cyber espionage, securing information systems and networks. As pointed out previously, cybersecurity in general – and cyberdefense in particular – have gained momentum due to increasing awareness of the potential that digital technologies offer for attacking, surveillance and meddling into national public affairs.

The revelations of NSA contractor Edward Snowden have been a particularly dire and palpable wakeup call for BRICS, with the Brazilian President's personal phone being wiretapped[93], together with the communications of a wide number of members of the Brazilian government[94], and Mr Snowden being in exile in Russia since the revelations.

In this perspective, as noted by Min Jiang's analysis in this book, cyberdefense and cybersecurity ultimately become instrumental to national sovereignty. The guarantee of network and information security and the capability to effectively defend critical infrastructure

[93] See Bridi & Greenwald (2013).

[94] See O Globo (2015).

are essential components of national security. As stressed by Jiang, this calculation drives BRICS countries – and arguably any other country – to prioritize their technological development and national control over information communication infrastructures. Indeed, the increasing interconnection and digitalisation of national economies, government services and virtually any “thing” imposes the necessity to be able to prevent, stop and manage cyberattacks, intrusions, theft, online distribution of harmful information.

Effective control and protection of critical infrastructures, information systems and databases are not only instrumental to assure cybersecurity but also national sovereignty. In this perspective, a number of states, most notably the Russian Federation[95], have argued that, to guarantee national sovereignty and cyberdefense, nation-states have the right to independently set policies regulating Internet critical resources, such as globally unique identifiers, including Internet Protocol (IP) addresses, domain names and autonomous system numbers that allow the Domain Name System (DNS) to smoothly function.

It is important to point out that, while it is absolutely legitimate for a country to exercise national sovereignty and set policies that apply both offline and online, such policies may contribute to the fragmentation[96] of the global Internet into national intranets and consequently their impact – with particular regard to the costs and benefits of the policies upholding sovereignty but fostering fragmentation – should be carefully considered by BRICS leaders.

To map the BRICS cyberdefense frameworks and provide the reader with a better understanding of the cyberdefense conceptualisations of these countries, the following elaborates our mapping in this area.

1.7.1 Cyberdefense Methodology

Scope

76. Is there a national cyberdefense strategy or is cyberdefense mentioned in the national defence strategy?

[95] See the Russian enactment of the “Internet Sovereignty” law, as highlighted by Andrey Shcherbovich’s analysis in chapter 4.

[96] In this perspective, see Drake, Cerf & Kleinwächter (2016).

77. What is the legal status of the national defence or cyberdefense strategy?

78. What national laws or other normative acts regulate cyberdefense in the country?

79. Is the country party of any international cooperation agreement in the sphere of cyberdefense?

80. Does the national cyberdefense strategy provide for retaliation?

Definitions

81. How are national security and national defence defined?

82. How are cybersecurity and cyberdefense defined?

83. How are threats to national security and cyberthreats defined?

84. How is a cyberattack defined?

85. Does the national law provide any other definitions instrumental to the application of cyberdefense legislation?

National framework

86. Is cyberdefense grounded on the constitutional provisions and/or international law?

87. Which specific national defence measures are related to cybersecurity?

88. Is there a national defence doctrine and does the law or strategy refer to it?

89. What measures are mentioned in the national law and strategy in order to implement cyberdefense?

90. How can Internet users' online activities be limited for the reasons of protection of national security and cyberdefense?

91. Does the national law or strategy foresee any special regime to be implemented in case of emergency in the context of cyberdefense?

92. Is there any specific framework regulating threats to critical infrastructure?

Actors

93. What actors are explicitly mentioned as playing a role regarding cyberdefense in the law or national cyberdefense strategy or defence strategy?

94. Is there a specific cyberdefense body?

95. What are the tasks of the aforementioned actors?

1.8 Towards Cooperation and Convergence in BRICS Cyber-policies

As stressed by the BRICS leaders themselves, ICTs "provide citizens with new tools for the effective functioning of economy, society and state [...] and the use and development of ICTs through international cooperation and universally accepted norms and principles of international law is of paramount importance in order to ensure a peaceful, secure and open digital and Internet space[97]." Since the Ufa Declaration, BRICS countries are prioritising digital policies in general and cybersecurity in particular in their own national agendas, while also pursuing increasing compatible cybersecurity objectives.

The Goa Declaration highlights the potential for cooperation amongst the BRICS countries that could "work together for the adoption of the rules, norms and principles of responsible behaviour of States including through the process of the United Nations Group of Governmental Experts (UNGGE)"[98]. Further, BRICS leaders established a BRICS Working Group on ICT Cooperation so that "members could actively lead and cooperate to strategize synergies, [...] sharing of information and case studies on ICT policies and programs in creating enabling environment"[99]. Moreover, a BRICS Science & Technology Enterprise Partnership (BRICS-STEP) was created, subsequently renamed STIEP, to highlight the importance of cooperation on mutually beneficial innovation and, as noticed in the introduction, the recent approval of the new BRICS STI Architecture, explicitly aims at improving the coordination of the BRICS STI cooperation governance structure, establishing and monitoring actions and involving a wide range of stakeholders "including policy makers, scientists, research organisations and a wider audience[100]."

[97] See BRICS. (9 July 2015).

[98] Ibid.

[99] Ibid.

[100] See BRICS (September 2019).

These initiatives make evident that BRICS have fostered both intergovernmental and multi-stakeholder cooperation. Importantly, BRICS countries have long recognized the value of multi-stakeholder partnerships to deal effectively with digital challenges, although of course each BRICS country may have a different perspective on how such partnerships must be implemented and what stakeholders should be involved. Over the past few years, BRICS have consistently affirmed that "the Internet is a global resource and that States should participate on an equal footing in its evolution and functioning, taking into account the need to involve relevant stakeholders in their respective roles and responsibilities[101]."

As mentioned previously, the Xiamen Declaration has clearly signalled the BRICS willingness to intensify intergovernmental cooperation to promote the "establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet[102]." In spite of not being formally organised into a specific intergovernmental organisation, BRICS countries do not need to start their policymaking cooperation from scratch, as they can rely on solid bases grounded in binding international agreements and joint membership of several intergovernmental organisations such as the United Nations system, the World Trade Organization, the International Monetary Fund and the World Bank. Common membership to all these organization provides more than one suitable arena for dialogue, cooperation and coordination, norm development and conflict resolution as well as exercise of global influence.

The existing solid diplomatic relations and international frameworks on which such relations rely have allowed BRICS countries to demonstrate that, while the countries remain a very elastic and heterogeneous grouping, they are capable of achieving impressive results with concrete actions, including creating an entirely new global financial institution such as the New Development Bank where their perspectives and interests align. Such BRICS activities reflect not only these countries' interest to rebalance the existing

[101] Ibid.

[102] See BRICS (2017).

international financial and economic architecture[103], but also their intention to develop convergent and legally interoperable digital policy frameworks.

The following chapters will present and map the five cybersecurity dimensions that have been introduced in the first chapter. Importantly, it can be argued that, even in the absence of formal cybersecurity agreements, the technological as well as regulatory, social and economic evolutions that BRICS countries are experiencing are triggering a process of spontaneous convergence in several sub-segments of the analysed dimensions. Such trends, which are already visible, deserve much more attention and scrutiny as we try to explore them in some detail in this volume[104].

Growing cooperation and legal interoperability amongst BRICS countries with regard to digital policy is increasingly possible and, to some extent, already happening. Given the importance and impact of BRICS digital policies for the entire world, it is the hope of the author of this chapter as founder and director of the CyberBRICS project that this volume will initiate much more needed research on such policies. Metaphorically, this book is laying the first brick on which CyberBRICS can be successfully built.

1.9 References

Antonakakis Manos *et al*. (2017). Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium August 16–18, 2017. Vancouver, BC, Canada <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf>.

Banga, Rashmi & Jeet Singh, Parminder (2019). BRICS Digital Cooperation for Industrialization. Working Paper 4/2019. Centre for Competition Regulation and Economic Development. University of Johannesburg.

Belli, Luca. (2017). Net Neutrality, Zero-rating and the Minitelisation of the Internet. Journal of Cyber Policy. Routledge. Vol 2. nº 1. <https://doi.org/10.1080/23738871.2016.1238954>.

Belli Luca. (2019). The Need for a RIoT (Responsible Internet of Things): A Human Rights Perspective on IoT Systems. In Mullen M. et al (2019). Navigating a New Era in Business and Human Rights. Institute of Human Rights and Peace Studies and Article 30. Pp. 181-188. <https://article30.org/wp-content/uploads/2019/08/a_new_era.pdf>.

[103] In this sense see Ziero (2015).

[104] The various facets of the BRICS digital policies will be analysed in the forthcoming works of the CyberBRICS project.

Belli, Luca. (2016). De la gouvernance à la regulation de l'Internet. Paris: Berger-Levrault.

Belli, Luca. (2015). A heterostakeholder cooperation for sustainable internet policymaking. Internet Policy Review, 4(2). <https://doi.org/10.14763/2015.2.364>.

Belli, Luca; Francisco, Pedro & Zingales, Nicolo. (2017). Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police. In Belli, Luca & Zingales, Nicolo (Eds.) Platform regulations: how platforms are regulated and how they regulate us. Rio de Janeiro. FGV Direito Rio. Pp 41-64. <https://bibliotecadigital.fgv.br/dspace/handle/10438/19402>.

Belli, Luca & Sappa, Cristiana. (2017). The Intermediary Conundrum: Cyber-regulators, Cyber-police or both? JIPITEC (Journal of Intellectual Property, Information Technology and Electronic Commerce Law) Special Issue: Intermediary Liability as a Human Rights Issue. Vol. 8, n° 3. Pp 183-198. <https://www.jipitec.eu/issues/jipitec-8-3-2017/4620>.

Belli, Luca & Venturini, Jamila. (2016). Private ordering and the rise of terms of service as cyber-regulation. Internet Policy Review, 5(4). <https://doi.org/10.14763/2016.4.441>.

Bond. (2019). Internet Trends 2019. <https://www.bondcap.com/report/itr19/#view/1>.

Boston Consulting Group (September 2017). Decoding the Chinese Internet. A white paper on China's Internet economy.

Brazilian Presidency of the BRICS. (2019). What is BRICS? <http://brics2019.itamaraty.gov.br/en/about-brics/what-is-brics>.

BRICS (October 2019). BRICS Science, Technology and Innovation Work Plan 2019-2022. <http://brics2019.itamaraty.gov.br/images/documentos/BRICS_STI_Work_Plan_2019-2022__Final.pdf>.

BRICS (September 2019). A New BRICS STI Architecture. <http://brics2019.itamaraty.gov.br/images/documentos/The_New_BRICS_STI_Architecture__Steering_Committee__Final_19_9_19.pdf>.

BRICS. (14 August 2019). Declaration of the BRICS Ministers of Science, Technology and Telecommunications, Brasilia, Brasil. <http://brics2019.itamaraty.gov.br/images/documentos/Declarao_da_5_Reunio_de_Comunicao_dos_Ministros_do_BRICS.pdf>.

BRICS. (July 2018). 10th BRICS Summit Johannesburg Declaration — BRICS in Africa: Collaboration for Inclusive Growth and Shared Prosperity in the 4th Industrial Revolution. July 25-27 2018, Johannesburg, South Africa. <http://www.brics.utoronto.ca/docs/180726-johannesburg.html>.

BRICS. (4 September 2017). 9th BRICS Summit. BRICS Leaders Xiamen Declaration. Xiamen, China. <http://www.itamaraty.gov.br/en/press-releases/17427-9th-brics-summit-brics-leaders-xiamen-declaration-xiamen-china-september-4-2017>.

BRICS. (16 October 2016). 8th BRICS Summit: Goa Declaration. Goa, India. <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/14931-viii-cupula-do-brics-goa-india-15-e-16-de-outubro-de-2016-declaracao-e-plano-de-acao-de-goa>.

BRICS. (18 March 2015). BRICS Memorandum of Understanding on Cooperation in Science, Technology and Innovation. Second BRICS Science, Technology and Innovation Ministerial Meeting. Brasília, 18 March, 2015. <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/8342-ii-reuniao-de-ministros-de-ciencia-tecnologia-e-inovacao-do-brics-documentos-aprovados-brasilia-18-de-marco-de-2015#mos>.

BRICS. (9 July 2015). Ufa Declaration, VII BRICS Summit. Ufa, Russian Federation. <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/10465-vii-cupula-do-brics-declaracao-de-ufa-ufa-russia-9-de-julho-de-2015#eng>.

BRICS Competition Centre. (2019). Digital Era Competition BRICS Report. <https://cyberbrics.info/digital-era-competition-brics-report/>.

BRICS STIEP WG. (May 2019). Minutes of the BRICS Working Group on Science Technology Innovation and Entrepreneurship Partnership (STIEP WG). Foz do Iguaçu, Brasil 12-15 May 2019. <http://brics2019.itamaraty.gov.br/images/documentos/Minutes_of_the_3rd_Meeting_of_the_STIEP_WG_-_Complete_version.pdf>.

BRICS Working Group on ICT Cooperation. (11 November 2016). Digital Partnership – Transformation through ICTs. ICT Development Agenda and Action Plan. 2nd Meeting of BRICS Ministers of Communications.

Bridi, Sonia & Greenwald, Glenn (1 September 2013). Documentos revelam esquema de agência dos EUA para espionar Dilma. O Globo. <http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html>.

Canongia, Claudia & Mandarino; Raphael. (2012). Cybersecurity: The new challenge of the information society. Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions. IGI Global.

Cisco. (2017). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2016 2021. White Paper. San Jose, CA: Cisco. <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html>.

Department of Telecommunications and Postal Services, South Africa. (2017). Cybersecurity Readiness Report 2017. <https://www.cybersecurityhub.gov.za/images/docs/Cyber-Readiness-Report.pdf>.

Dewar, Robert S. (Ed.) (2018) National Cyberdefense Policy Snapshots. Cyber Defence Project (CDP). Zürich, September 2018. Centre for Security Studies (CSS).

Drake, William J.; Cerf Vinton G. & Kleinwächter, Wolfgang. (January 2016). Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper. <http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf>.

Ewing, Reese. (27 July 2016) Brazil prosecutor freezes $11.7 million of Facebook funds due to WhatsApp case. Reuters. <https://www.reuters.com/article/us-brazil-facebook-whatsapp-idUSKCN10801Q>.

European Union Chamber of Commerce in China (2019). The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors. <https://www.europeanchamber.com.cn/en/publications-archive/709/The_Digital_Hand_How_China_s_Corporate_Social_Credit_System_Conditions_Market_Actors>.

Fichtner, L. (2018_). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review, 7*(2), 1-19. <https://doi.org/DOI:10.14763/2018.2.788>.

Gemalto. (2018). Breach Level Index. <https://breachlevelindex.com/request-report>.

Kolomychenko, Maria. (30 August 2018). Russia tries more precise technology to block Telegram messenger. Reuters. <https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ>.

Kunming. (11 September 2019). Kunming enhances technology cooperation with BRICS countries. <http://en.kunming.cn/c/2019-09-11/10793655.htm>.

Kiselev, Vladimir & Nechaeva, Elena. (2018). Priorities and Possible Risks of the BRICS Countries' Cooperation in Science, Technology and Innovation, 5(4) BRICS Law Journal 33–60 <https://doi.org/10.21684/2412-2343-2018-5-4-33-60>.

Kuneva, Meglena. (31 March 2009). Keynote Speech. Rundtable on Online Data Collection, Targeting and Profiling. Brusseks, European Commission. <http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm>.

Marzano, Artur *et al.* (2018). The Evolution of Bashlite and Mirai IoT Botnets. in 2018 IEEE Symposium on Computers and Communications (ISCC). <https://ieeexplore.ieee.org/document/8538636>.

Mosenia, Arsalan & Jha, Niraj K. (2016). A Comprehensive Study of Security of Internet-of-Things. in IEEE Transactions on Emerging Topics in Computing. Vol. 5 N° 4 <https://ieeexplore.ieee.org/document/7562568>.

NIST (National Institute of Standards and Technology) (August 2003). Special Publication 800-59. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf>.

ICCPR (International Covenant on Civil and Political Rights). (1966). Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966 entry into force 23 March 1976. <https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>.

Itamaraty. (27 June 2019). BRICS Informal leaders' meeting on the margins of the G20 Summit – Joint Media Statement – Osaka, 28 June 2019. <http://www.itamaraty.gov.br/en/press-releases/20557-brics-informal-leaders-meeting-on-the-margins-of-the-g20-summit-joint-media-statement-osaka-28-june-2019>.

ITU. (2016). Harnessing the Internet of Things for Global Development: A Contribution to the.

ITU. (2014) Understanding cybercrime: Phenomena, challenges and legal response Geneva: ITU Telecommunication Development Bureau. <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf>.

ITU. (2005). ITU WSIS Thematic Meeting on Cybersecurity. Chairman's Report. ITU Headquarters, Geneva, Switzerland. 28 June – 1 July 2005.

ITU-T. (2009). Recommendation X.1205 (04/08): Overview of cybersecurity. Approved in 2008-04-18. <https://www.itu.int/rec/T-REC-X.1205-200804-I>.

UN Broadband Commission for Sustainable Development. Geneva: International Telecommunication Union. <https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf>.

O Globo. (4 July 2015). EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeak. <http://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html>.

O'Neill, Jim. (November 2001). Building better global economic BRICs. New York: Goldman Sachs. Global Economics Paper, n. 66. <http://www.goldmansachs.com/our-thinking/archive/archive-pdfs/build-better-brics.pdf>.

Pankov, Nikolay. (19 March 2019). Mirai goes Enterprise. Karspersky Daily. <https://www.kaspersky.com/blog/mirai-enterprise/26032/>.

Sanger, David E. & Perlroth, Nicole. (June 15, 2019). U.S. Escalates Online Attacks on Russia's Power Grid. <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html?smid=nytcore-ios-share>.

Sevastopulo, Demetri & Bond, David. (17 February 2019) UK says Huawei is manageable risk to 5G. Financial Times. <https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5>.

Statista. (2019). Number of smartphone users by country as of September 2019 (in millions). <https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/>.

Stuenkel, Oliver. (2016). Post-Western World: How Emerging Powers Are Remaking Global Order. Polity Press.

The Economist. (6 May 2017). The world's most valuable resource is no longer oil, but data. <https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>.

UNCTAD (United Nations Conference on Trade and Development). (2016). Data protection regulations and international data flows: Implications for trade and development. <https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>.

United Nations' High Level Panel on Digital Cooperation (2019). The Age of Digital Interdependence: Report of the High-Level Panel on Digital Cooperation. <https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf>.

UNGA (United Nations General Assembly). (1 March 2018). Progress made in the implementation of and follow-up to the outcomes of the World Summit on the Information Society at the regional and international levels. Report of the Secretary-General. A/73/66–E/2018/10.

UNODC (United Nations Office on Drugs and Crime). (2013). Comprehensive Study on Cybercrime. Vienna: UNODC. <https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf>.

Vaidya, Tavish. (July 2015). 2001-2013: Survey and Analysis of Major Cyberattacks. Department of Computer Science, Georgetown University. <http://arxiv.org/pdf/1507.06673.pdf>.

WEF. (January 2011). Personal Data: The Emergence of a New Asset Class. <http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf>.

Wolff, J. (2016). What we talk about when we talk about cybersecurity: Security in internet governance debates. Internet Policy Review, 5(3). <https://doi.org/doi:10.14763/2016.3.430>.

World Bank. (2016). World Development Report 2016: Digital Dividends. Washington, DC: World Bank. <http://pubdocs.worldbank.org/en/391452529895999/WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf>.

World Bank (2017). Combatting Cybercrime Tools and Capacity Building for Emerging Economies. Washington, DC: The World Bank. <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/worldbank-combating-cybercrime-toolkit.pdf>.

Ziero, Gabriel Webber. (December 2015). Looking for a BRICS perspective on international law. Revista de Direito Internacional, Brasília. Vol. 12. N. 2. Pp. 303-322. <https://doi.org/10.5102/rdi.v12i2.3678>.

XinhuaNet. (7 August 2019). BRICS set up new institutional branch to strengthen cooperation on ICT. <http://www.xinhuanet.com/english/2019-08/07/c_138289903.htm>.