DIGITAL DIALOGUE

Brazil's Cyber Resilience and Diplomacy: The Place for Europe

Hannes Ebert and Laura Groenendaal
The German Marshall Fund of the United States
April 2020

EU CYBER DIRECT
Supporting EU Cyber Diplomacy

This project is funded by the European Union.

Contents

Abstract

Brazil is a critical partner for the EU in its efforts to build a secure and rights-based global cyberspace. It has made significant advances in digitization domestically and played a pivotal role in international negotiations on cyber security and data protection. At the same time, Brazil is facing mounting challenges related to cyberspace. Concerns have arisen regarding issues of internet freedom, data protection, net neutrality, and disinformation. The country has also been confronted with an increasing number and sophistication of cyber threats. Brazil's ability to exploit the benefits of the evolving digitization while mitigating these risks will strongly influence the dynamics of its cyber partnership with the EU. To identify areas of mutual interest in cyber security and diplomacy between Brazil and the EU, this Digital Dialogue paper provides an overview of Brazil's cyber ecosystem, illustrates its legislative, institutional and strategic cyber security policies, assesses its positions in regional and global cyber security debates, and outlines the evolution of Brazil-EU cyber cooperation. As Brazil assumed the chairmanship of the sixth United Nations Group of Governmental Experts (UNGGE) established in December 2018, this paper also discusses both sides' positions in these negotiations. The study draws on publicly available primary and secondary sources as well as interviews with officials and experts conducted in Brasilia and São Paulo in May 2019.

Key points

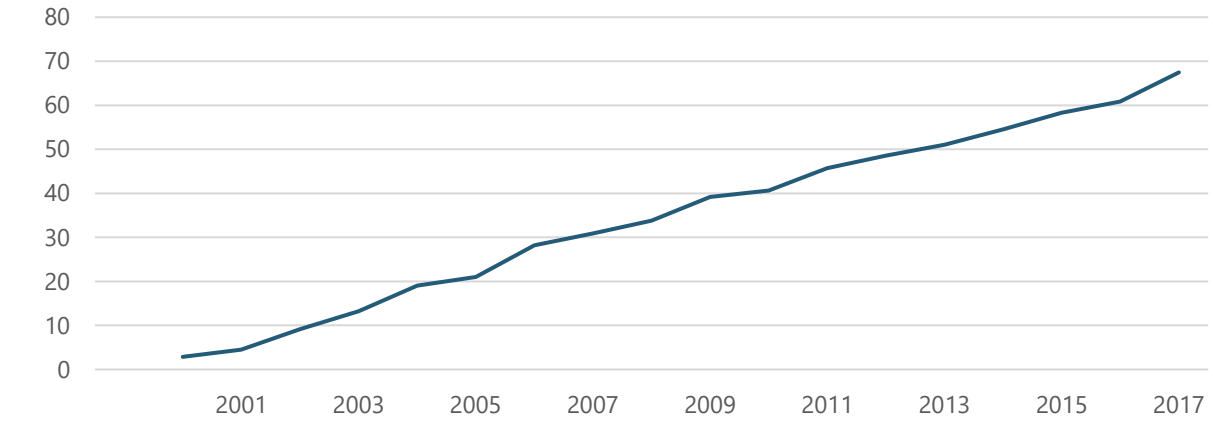
- Successive Brazilian governments' legislative, institutional and strategic reforms to exploit the benefits of emerging technologies while mitigating their risks continue to be a highly contentious political issue. While Brazil's 2014 Marco da Civil was applauded as a benchmark for digital rights, its efforts to secure the FIFA World Cup in 2014 and the Olympic Games in 2016 as well as measures to curb disinformation sparked criticism by groups advocating internet freedom and privacy. As Brazil develops a new national cyber security strategy and establishes a new federal data protection agency, these political struggles will persist.
- As Latin America's largest technology hub and the world's fourth largest internet user base, Brazil has become a top target of transnational cyber crime, the primary cyber threat to its users and networks. Its accession to the Budapest Convention, initiated in December 2019 after years of reluctance, will offer a mechanism to address the challenge internationally.
- Brazil's ability to walking a diplomatic tightrope in international debates on norms of responsible state behavior and data privacy will be tested in 2020, as it will be compelled to make hard choices regarding 5G and global cyber crime regulations and navigate a polarized setting chairing the UNGGE. Amidst a technological standoff between China and the US, Brazil is positioning itself as bridge builder.
- A broadened and widened partnership with the EU on ICT and research, internet governance, cyber crime and cyber norms will become increasingly essential to maintain a stable and rules-based cyberspace. Brasília and Brussels should invest in enhanced information sharing, public documentation of how international law applies and joint capacity building, efforts that require involving multiple stakeholders.

1. General country profile

Brazil is a critical partner for the EU in its efforts to build a secure and rights-based global cyberspace. It is the world's eighth largest economy by GDP, and by far South America's most populous and powerful state.[1] Despite economic and political crises since 2014, it has made significant advances in domestic digitization and played a pivotal role in international negotiations on cyber security and data protection. Brazil has the world's fourth largest internet user base, after China, India and the US and before Japan.[2] The share of Brazilians using the internet has increased from less than 3 percent of the population in 2000 to an estimated 67.5 percent in 2017 (see figure 1).

The Brazilian federal government has launched several programs since 2010 to expand and improve internet services, including the National Broadband Plan (*Plano Nacional de Banda Larga*, PNBL) to deliver affordable broadband connections to municipalities across the country. Hosting the FIFA World Cup in 2014 and the Summer Olympics in 2016, the Brazilian authorities increasingly invested in broadband connections and the transition from 3G to 4G networks.[3] In 2017, Brazil started public consultations for a new national connectivity plan called Internet for All (*Internet para Todos*) to increase internet access and boost fixed and mobile broadband infrastructure in the country.[4] That same year, the country launched its first defence and strategic communications satellite to provide secure communication channels for defence purposes and enhanced broadband capacity. Overall, Brazil is one of Latin America's major telecommunications markets. Its market has been dominated by a small number of large private companies, with Vivo, TIM, Claro, and Oi holding almost 98 percent of the mobile market already in 2014.[5]

Figure 1. Brazil's Internet Usage, 2000-2017



Source: Internet Live Stats, "Internet Users by Country". 2019, available at http://www.internetlivestats.com/internet-users-by-country/

[1] For most recent GDP figures in 2017, see The World Bank, GDP (current US$), 2019, available at https://data.worldbank.org/indicator/ny.gdp.mktp.cd?most_recent_value_desc=true.

[2] Internet Live Stats, "Internet Users by Country". 2019, available at http://www.internetlivestats.com/internet-users-by-country/. The data on internet users is estimated for 2016; for data on 2017, see International Telecommunications Union, "Brazil profile", 2018, available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx.

[3] Gustavo Diniz, Robert Muggah and Misha Glenny, "Deconstructing Cyber Security in Brazil: Threats and Responses", Igarape Institute, 2014, p.7, available at https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf.

[4] Freedom House, "Brazil", 2018, available at https://freedomhouse.org/report/freedom-net/2018/brazil.

[5] International Telecommunication Union, Measuring the Information Society Report Volume 2. ICT Country Profiles, Geneva: ITU, 2018, p. 26, available at https://www.itu.int/en/ITU-D/Statistics/Pages/publications/misr2018.aspx.

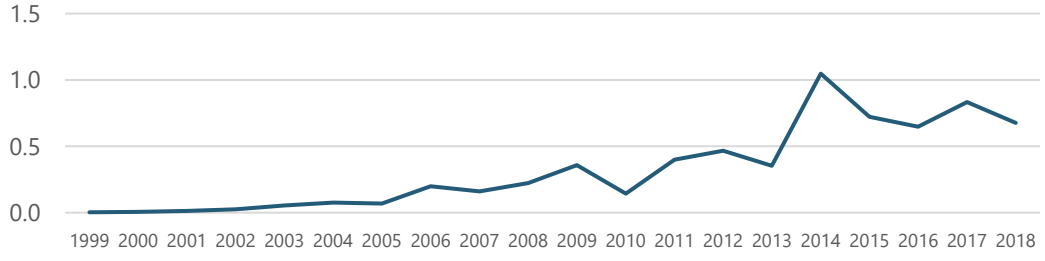
The Brazilian state has taken significant steps to regulate Brazil's digital transformation. In 2014, according to one account, there had been over 1,000 internet-related bills under consideration by the Brazilian National Congress.[6] Most importantly, the Marco Civil da Internet (MCI, also known as the Brazilian Internet Bill of Rights or the Brazilian Civil Rights Framework), a comprehensive rights bill approved in 2014 to set norms on net neutrality, freedom of expression and privacy, was the first of its kind in the world and widely perceived as a benchmark for digital rights. Since then, issues of internet freedom, data protection, and net neutrality have been highly contested among the multiple stakeholders. More recently, concerns about disinformation emerged during the general elections in 2018 and led to a set of legislative actions and public debate (for more details, see section 2.3.2).

Brazil has also been confronted with an increasing number and sophistication of cyber threats. The number of computer incidents reported to Brazil's Computer Emergence Response Team (CERT.br) grew from 3,107 in 1999 to 676,514 in 2018, with a peak of over 1 million in 2014, when Brazil hosted the FIFA World Cup (see figure 2). Cybercrime has constituted Brazil's main cyber threat, and the country has consistently topped global cybercrime rankings. In 2017, around 60 million adults in Brazil experienced cybercrime. That year, Brazilian consumers lost an estimated $22.5 billion, an amount only surpassed by China.[7] In 2015, more than half of all cyberattacks in Brazil reportedly originated domestically.[8] Economically motivated cybercrime in the field of online banking fraud and financial malware is particularly significant in this regard, which can be explained by Brazil's large electronic banking service sector. In 2017, Brazil was also the world's fifth worst botnet-infected country.[9]

Cybercrime attacks have not only targeted government agencies and large organisations but also citizens and small and medium-sized businesses. The Brazilian authorities reported more than 100,000 instances of internet-related fraud in 2016, although the real number is estimated to be higher.[10] Apart from cybercrime, Brazilian public and private networks have also been targeted for political purposes. For example, in 2013, the hacktivist group *Anonymous Brazil* successfully targeted websites of media groups and the Brazilian Intelligence Agency (ABIN). In 2016, these attacks reached a new high when *Anonymous Brazil* launched a series of distributed denial-of-service (DDoS) attacks on state and municipal websites in the run-up to the 2016 Olympic Games.

Figure 2. Computer incidents reported to CERT.br annually

1990-2018, million



Source: CERT.br, *Estatísticas dos Incidentes Reportados ao CERT.br*, 2019, available at https://www.cert.br/stats/incidentes/[11]

[6] Diniz, Muggah and Glenny, p. 20. The study draws on data by the Observatório da Internet no Brazil, a project run by the Brazilian Internet Steering Committee (CGI.br).

[7] Ibid.

[8] Norton, Norton Cyber Security Insights Report 2017 Global Results, 2017, available at https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf.

[9] Robert Muggah and Nathan Thompson, "Brazil struggles with effective cyber-crime response", Jane's Intelligence Review, 2017, available at https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf.

[10] Ibid.

[11] CERT.br collects and published data on cyber incidents. Notifications on incidents are voluntary.

Brazil's ability to exploit the benefits of the evolving digitization while mitigating these risks will strongly influence the dynamics of its cyber partnership with the EU. To identify areas of mutual interest in cyber security and diplomacy between Brazil and the EU, this Digital Dialogue paper provides a general overview of Brazil's cyber ecosystem, illustrates its legislative, institutional and strategic cyber security policies, assesses its international and regional positions, and outlines the evolution of Brazil-EU cyber cooperation. As Brazil assumed the chairmanship for the sixth United Nations Group of Governmental Experts (UNGGE) established by the UN General Assembly in December 2018, this paper also discusses both sides' positions in these negotiations. The study draws on publicly available primary and secondary sources as well as interviews with officials and experts conducted in Brasilia and São Paulo in May 2019.

2. General evolution of the cyber security sector

2.1. Legal and regulatory landscape

2.1.1. Cyber security policy directives and strategy

Table 1 provides an overview of the five policy documents that have primarily shaped Brazil's strategic framework on cyber security. While these documents cover cyber strategies and cyber security policy at large, the following sections focus specifically on data protection and digital rights, cybercrime legislation and cyber resilience and infrastructure policies.

Table 1. Brazil's main cyber policy documents

Year	Name	Initiating actor	Summary
2008	National Defence Strategy	Ministry of Defence	Divides national defence into the three strategic sectors of space, nuclear and cyber. The army takes charge of the cyber sector.
2010	Green Book on Cybersecurity	Department of Information and Communication Security (DSIC), Presidential Office for Institutional Security Cabinet (GSI-PR)	Identifies basic organisational principles and elevates the office of the presidency's cyber responsibilities. Did not yet outline any clear co-ordination mechanisms regarding political, strategic, and operational matters.
2012	Defence White Paper	Ministry of Defence	Updated version of 2008 strategy that further develops doctrinal proposals on cyber security and established the Ministry of Defence's Cyber Defence Centre.
2015	Information and Communications Security and Cyber Security Strategy of the Federal Public Administration	GSI-PR	Describes measures to secure federal public administration networks from cyberattacks for the time period from 2015 to 2018.
2018	Brazilian Digital Transformation Strategy (E-Digital)	Department of Digital Transformation Policy, Ministry of Science, Technology, Innovations and Communications	Integrates the various governmental initiatives on digital issues within one framework and suggests 100 strategic actions to be implemented within four years.
2018	National Policy of	Casa Civil, Presidency	Suggests steps to guarantee the national

Year	Name	Initiating actor	Summary
	Information Security (PNSI)		availability, integrity, confidentiality and authenticity of information.
Tbc, submitted for public consultation in late 2019	National Cyber Security Strategy	GSI-PR	Outlines national cyber security priorities regarding the national cyber security governance, prevention and mitigation of cyber threats, and strategic protection, across the areas of legal and regulatory measures, international and strategic partnerships, research, development and innovation, and education.

2.1.2. Data protection and privacy rights

In 2014, after several years of consultations (2009-2012) and drafting (2012-2014), Brazil passed the **Marco Civil da Internet** (MCI). The law was developed by the Brazilian Congress in cooperation with multiple stakeholders and has been widely considered a landmark document for advancing digital rights.[12] The MCI drafting process was initiated in reaction to a controversial bill on cybercrime (Bill 84/1999, also known as the Lei Azeredo), proposed by Representative Luiz Piauhylino in 1999 and amended by Senator Eduardo Azeredo in 2006, to criminalize a range of online practices. Legal scholars and civil society activists strongly mobilized against the approval of the bill, opposing the broad definition of crimes and the disproportionality of some suggested criminal penalties, and asserting that cybercrime legislation should be based on a broader civil regulatory framework. This opposition reflected increasing public advocacy for greater digital rights, universal access and net neutrality and against the tightening of government and military control over cyberspace.[13]

At the invitation of Ministry of Justice officials including Danilo Doneda and Laura Schertel, a group of experts, most prominently Ronaldo Lemos, then at the Fundação Getulio Vargas (FGV)'s Centre for Technology and Society (CTS), proceeded to create an online multistakeholder, public consultation process between 2009 and 2010.[14] The process was also inspired by a set of ten Principles for the Governance and Use of the Internet approved and promoted by the Brazilian Internet Steering Committee (*Comitê Gestor da Internet no Brasil*, CGI.br) in 2009.[15] After delays related to the election of President Dilma Rousseff in 2010 and concomitant deadlocks in the government, the agreement resulting from this process was sent as a Bill of Law to the National Congress in 2011.

[12] The following observations are based on interviews with data protection experts in São Paulo and Brasilia between June 2-7, 2019. For an overview of the evolution of Marco Civil, see Carlos Affonso Souza, Fabro Steibel and Ronaldo Lemos, "Notes on the creation and impacts of Brazil's Internet Bill of Rights", The Theory and Practice of Legislation, 5:1, 2017, pp. 73-94. Compare also Anri van der Spuy, What if we all governed the Internet? Advancing multistakeholder participation in Internet governance, Paris: UNESCO, 2017, p. 44-51. For a brief legal discussion on data protection and privacy in Brazil, see Mattos Filho and Veiga Filho, Data Security and Cybercrime in Brazil, Lexology, October 29, 2018, available at https://www.lexology.com/library/detail.aspx?g=a1b949b5-5644-4941-858e-96c983ca7e42. In addition, more detailed background information is provided in the research of the FPI's project on data protection implemented by B&S Europe.

[13] Muggah and Thompson 2017.

[14] Lemos was the first to frame the initiative as "Marco Civil". In May 2007, as a response to debates on the draft Lei Azeredo, he argued that "instead of a criminal bill, Brazil should have a 'civil rights framework' for the Internet or, in other words, a 'Marco Civil'" (Ronaldo Lemos, "Internet Brasileira Precisa da Marco Regulatório Civil", Folha de São Paulo, Ma 22 2007, available at http://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm)

[15] The list of principles can be found at CGI, Principles for the governance and use of the Internet, 2009, available at https://www.cgi.br/resolucoes-2009-003-en/. Principles range from freedom, privacy and human rights to a democratic and collaborative governance and network neutrality.

Subsequently, various subjects such as net neutrality and copyright but also data protection, liability and privacy were debated. Among the most vocal opponents to the initial draft were telecommunication companies, who - with support from pro-business parliamentarians such as Eduardo Cunha - rallied against rules on net neutrality and intermediary liability. Large public demonstrations, demanding inter alia enhanced public participation in policy-making, and substantial media attention around leaked classified documents by then-US intelligence contractor Edward Snowden on the US National Security Agency's (NSA) phone tapping of top Brazilian government officials and collection of Brazilians' communications data in 2013 propelled the legislative process forward.[16] A revised and more comprehensive version of the initial draft was approved by the Brazilian Congress and Senate in April that year and adopted as Law no. 12965 in June 2014. The legislation upheld a broad set of protection rights ranging from net neutrality and freedom of expression to privacy guarantees, and sought to enact safeguards against mass surveillance. The bill also guaranteed the inviolability and secrecy of online communications of users, allowing exceptions exclusively by court order, and created safe harbours for Brazilian intermediaries, which without a judicial order to delete specific content, would not be liable for content published by third parties.[17]

However, controversial debates persisted during the MCI's implementation phase, and its provisions have been challenged in Brazilian courts, with observers noting that it lacked "a strong, well-defined data protection system".[18] Between 2014 and 2016, the government, private sector and civil society negotiated a general data protection law. Four rounds of online multistakeholder consultations took place in 2015. While the private sector was increasingly supportive of a law focused on data protection, the Ministries of Planning and Economy (now merged into one) feared that it would weaken the competencies they held under the then-existent consumer protection regime. In addition, Congress in parallel considered legislation to reinforce anti-cybercrime measures that would have rolled back key MCI provisions, including on compelling multinational internet companies to store data locally on servers in Brazil (2014), on blocking the instant messaging platform WhatsApp (2015), and on increasing government surveillance capabilities (2016).[19] Separately, during the negotiations, the Federal Police insisted on a clause that would make data registries mandatory for ISPs, to be used for investigations and forensics in cybercrime cases.[20] These competing measures illustrate the political sensitivities and challenges in developing strong user data privacy protections and public security policies.

On May 11, 2016, only one day before the Senate voted to suspend President Rousseff's powers following her impeachment in mid-April, Rousseff enacted the **Presidential Decree no. 8711/2016**, a draft bill which listed the exceptions to net neutrality, inhibited the practice of unilateral conducts or agreement jeopardizing the public and unrestricted nature of the internet and restricted personal data collection, and specified the modalities of governance of the internet framework, including authorities entitled to enforce legislations. The bill was a compromise as it excluded, for example, a reference to a data protection authority, which was opposed by the Ministry of Planning. As such, it was approved unanimously by Congress and Senate and came into force on June 10, 2016. While some of the

[16] See Tiago Pedro Vales, "Brazil´s cyberspace politics: Combining emerging threats with old intentions", IAPSS, Vol.29, October 2014, p. 303, available at https://iapss.org/wp-content/uploads/2014/10/295_Volume-29.pdf. Also cp. Adriana Abdenur and Carlos da Silva Gama, "Triggering the Norms Cascade: Brazil's Initiatives for Curbing Electronic Espionage", Global Governance, 21:3, pp. 455-474.

[17] Phone interview with a civil society representative, December 3, 2018. See also Gabriel Aleixo et al., The Encryption Debate in Brazil, Washington DC, Carnegie Endowment, 2019, p. 4, available at https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219.

[18] Muggah and Thompson 2017, p. 5.

[19] These legislative efforts will be discussed in section 2.3.3 on cybercrime and cyber defence.

[20] Diniz, Muggah and Glenny 2014, p.21. The question on how long ISPs and content providers should maintain connection registers for review of Brazilian authorities was highly contested.

provisions such as the Congress's competence to establish a government authority were legally controversial, it intentionally sent a strong political message.

After Rousseff's impeachment, a new coalition of members of the National Congress and Senate were eager to adjust MCI, which was associated with the previous government.[21] However, the Cambridge Analytica data sharing scandal during the 2016 US elections, Brazil's aspirations to join the Organization for Economic Co-operation and Development (OECD), and Europe's passage of the General Data Protection Regulation (GDPR) strongly drove further legislation. An alliance between the civil society and private sector, in particular foreign companies, on promoting data protection legislation evolved and led to the formation of two coalitions: the Rights on Networks Coalition (*Coalizão Direitos na Rede*), which comprised of left-wing political parties and various civil society actors such as Article 19, Coding Rights, the Brazilian Institute for Consumer Protection (*Instituto Brasileiro de Defesa do Consumidor*, IDEC), FGV Law School and ITS, and the Brazilian Association of Information and Communication Technology Companies (*Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação*, BRASSCOM).[22] As a result, on August 15, 2018, the Brazilian Congress passed the **General Data Privacy Law** (*Lei Geral de Proteção de Dados Pessoais*, LGPD), Brazil's first comprehensive legislation specifically addressing data protection.[23] As the law is largely aligned with the EU's GDPR, including significant extraterritorial application and high fines for defiance, it makes Brazil one of the few jurisdictions with a data privacy protection system comparable to that in the EU.[24]

On December 14, 2018, outgoing President Temer issued an Executive Order that made significant changes to the LGPD, most notably creating the Brazilian National Data Protection Authority (*Autoridade Nacional de Proteção de Dados*, ANPD) to oversee and enforce the LGPD and placing it in the Presidency's remit. It also changed the LGPD's enforcement date from February 2020 to August 2020 to allow Brazilian entities more time to comply with the new law.

2.1.3. Cybercrime legislation and its compatibility with the Budapest Convention

In Europe, the 2001 *Council of Europe's Convention on Cybercrime* (the **Budapest Convention**) is widely seen as the key instrument to harmonize its signatories' cybercrime legislations and to develop a joint judicial area for cyberspace more generally. By 2019, 67 states had signed the convention, inlcuding 26 non-members of the Coucil of Europe. Brazil, however, refrained from joining the convention (Japan and the United States, among others, have signed the convention as non-members, while China, India, Russia and South Korea have not) and has repeatedly expressed scepticism.[25] Although Brasilia has not contested the convention's general legislative rationale and even used it as a template for reforming domestic legislation, it denounced the treaty as discriminatory, as it was not

[21] Souza, Steibel and Lemos, 2017, p. 89.

[22] Interview with senior legal scholar, June 6, 2019, Brasilia, Brazil. For more information, see the webpages of the Rights on Network Coalition, available at https://direitosnarede.org.br/, as well as of BRASSCOM, available at https://direitosnarede.org.br/.

[23] The bill was approved by the Chamber of Deputies and then, in a rare unanimous vote, adopted by the Senate. The following observations are based on interviews with data protection experts in São Paulo and Brasilia, June 2-7, 2019. For additional commentary, see Melanie Ramey, "Brazil's New General Data Privacy Law Follows GDPR Provisions", 2018, Inside Privacy, available at https://www.insideprivacy.com/international/brazils-new-general-data-privacy-law-follows-gdpr-provisions/.

[24] One observer notes that "(t)he legislation - similar to the General Data Protection Regulation (GDPR) - creates a new legal framework for the use of personal data processed on or related to individuals in Brazil, regardless of where the data processor is located" (Chris Brook, "Breaking Down LGPD, Brazil's New Protection Law", DataInsider, June 10, 2019, available at https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law). For a comparison between LGPD and GDPR, see Bruno Bioni, Maria Gomes, and Renato Monteiro, "GDPR matchup: Brazil's General Data Protection Law", IAPP Privacy Trackers, October 4, 2018, available at https://iapp.org/news/a/gdpr-matchup-brazils-general-data-protection-law/.

[25] Annegret Bendiek, Tests of Partnership: Transatlantic Cooperation in Cyber Security, Internet Governance and Data Protection, 2014, Policy Paper, Washington DC: Transatlantic Academy, p. 10.

part of its original drafting process (a concern it has expressed jointly with India), and more generally as biased toward the West.[26] However, further to a request for accession, the Council of Europe invited Brazil to acceede to the convention in December 2019; once internal procedures to become a party are completed, Brazil will thus eventually become a party and a priority country for capacity building programs.[27]

While successive Brazilian governments have been reluctant to sign the Budapest Convention, Brazil has been increasingly active in shaping domestic and international norms on cybercrime. At the domestic level, as outlined above, parts of the legislation on cybercrime came into conflict with legislation on privacy and data protection.[28] The congressional opposition's repeated attempts during President Rousseff's presidency to develop more forceful cybercrime laws that would allow for more intrusive measures, such as provisions for government and police to access data without judicial order, were in line with the preferences of law enforcement agencies. Two of the first laws specifically addressing cybercrime came into force in 2013: Law 12.735 and Law 12.737.[29] Law 12.735, also known as the **Azeredo Bill** (Lei Azeredo), constituted a general modification of the penal code to specify electronic crimes. The law sanctioned augmented penalties for crimes against public figures such as politicians. As outlined above, various provisions of the Azeredo Bill were considered a violation of privacy rights and enabling government overreach, and opposition to the bill was a main driver for drafting the MCI. However, intimate photos of actress Carolina Dieckmann released online without consent and ensuing media coverage prompted the passage of of the bill. Relatedly, law 12.737, also popularly known as the **Law Carolina Dieckmann**, constituted Brazil's first amendment of the Brazilian Penal Code that entailed norms that categorized and specified penalties for different types of cybercrimes, which was previously not covered by criminal law. It introduced two articles to the Penal Code that for the first time made unauthorized access of computer devices a criminal offense.[30] Similar to the Azeredo Bill, it was enacted in 2013, one year before the MCI.[31]

In February 2015, bill **PL 215/2015** suggested amending the Penal Code to increase the penalty for crimes against honour (slander, libel and defamation) practiced in social networks and oblige internet companies to store user information and provide it to law enforcement without a court order. It also sought to introduce an internet registry to collect users' personal data. The bill, complemented by three additional amendments throughout 2015, became increasingly opposed by privacy rights advocacy groups and dubbed "the **spy bill**" (PL Espião in Portuguese). It was ruled as constitutional by

[26] Thomas Renard, "EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain," European Politics and Society, 28 January 2018, p. 12-13, available at http://www.egmontinstitute.be/content/uploads/2018/01/EPS-EU-cyber-partners_RENARD_AM.pdf?type=pdf. See also Diniz, Muggah and Glenny 2014, p. 27.

[27] Council of Europe, "Budapest Convention: Brazil invited to accede", 2019, available at https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede.

[28] On the legal aspects of cybercrime, including what activities constitute cybercrime and what penalties, see Daniel de Souza, Brazil: Cybersecurity 2019, 2018, available at https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/brazil.

[29] Daniel Arnaudo, Brazil, the Internet and the Digital Bill of Rights, Strategic Paper 25, Rio de Janeiro: Igarapé Institute, 2017, pp. 11-13.

[30] Renato Opice Blum, "New Brazilian Cyberlaw", Council of Europe Blog, April 17, 2013, available at https://www.coe.int/en/web/octopus/blog/-/blogs/new-brazilian-cyberlaw. Some observers argued that its impact was marginal as the penalties for criminal activities were, also in comparison to US and EU legislation, to weak to deter; see Robert Muggah and Nathan Thompson, "Brazil's Cybercrime Problem", Foreign Affairs, September 17, 2015, available at https://www.foreignaffairs.com/articles/south-america/2015-09-17/brazils-cybercrime-problem.

[31] Omar Kaminski, "Cybercrime in Brazil", in Eduardo Magrani (Ed.), "Digital Rights: Latin America and the Caribbean", FGV Direito Rio, 2017, pp-228-229, p.228. Previously, other provisions such as a law from 1996 addressing telematics interception and a law from 2000 containing provisions on public administration had been applied to cyberspace.

the Commission of Constitution and Justice but did not pass before President Temer came into office in August 2016.[32]

Furthermore, in May 2016, the Inquiry Parliamentary Commission on Cybercrime (**CPICiber**), created in July 2015 by then-President of the Chamber of Deputies Eduardo Cunha, approved its final report that introduced seven bills to enhance measures against cybercrime. These measures ranged from facilitating access to internet protocol (IP) numbers by investigative authorities to rules on intermediary liability. The report provoked substantial opposition domestically and internationally. Digital rights activists criticized that the proposals would undermine the MCI's provisions, provide draconian powers for law enforcement agencies, roll back safeguards for freedom of expression and privacy and peel back the right to anonymity. The opposition warned that one of the proposals could force ISPs to release users' names and other personal information associated with an IP address without requiring a judicial order, while another would allow for internet services such as Facebook or WhatsApp to be blocked by judicial order.[33] The report was also opposed by an international campaign, with the founder of Facebook, Mark Zuckerberg, supporting a petition against what he perceived as a threat to free internet in Brazil.[34] At the time of writing, these initiatives still had to be approved.

2.1.4. Cyber resilience and critical infrastructure protection

Beyond the cyber security doctrines listed in table 3, Brazil has taken several regulatory steps specifically focused on the protection of its critical information infrastructure. An **Ordinance** promulgated by the GSI-PR on February 8, 2008 established the still valid definition of critical infrastructure in Brazil: "IEC [Critical Infrastructures] are considered as installations, services and goods that, if disrupted or destroyed, will have serious social, economic, political, international or national security impact".[35] The Ordinance's article 2 also established technical groups for security of critical infrastructures and other measures. Article 3 identifies energy, finance, telecommunications, transport network, and water as priority areas of critical infrastructure protection. There is no whole-of-government document that exclusively addresses the more specific issue of critical information infrastructure protection (CIIP). Instead, the issue is covered by various strategic documents on civil defence and digital transformation as well as legal references such as the abovementioned strategic documents and cybercrime legislation.

To minimize the risk related to its **supervisory control and data acquisition** (SCADA) system, through which most of its critical infrastructure is managed, the federal government established several critical infrastructure technical groups in 2008, 2009, and 2014, including among others the ministries of defence, foreign affairs, health, and science and technology, the central bank, as well as private sector representatives, to develop recommendations for increasing SCADA management effectiveness.[36]

[32] A key architect of this bill is the former president of Brazil's lower house of Congress, Eduardo Cunha, who was a leading opponent of the Marco Civil and teamed up against the bill with the Congress's evangelical caucus. See Robert Muggah and Nathan B. Thompson, "Brazil's Digital Backlash", NYT, 12 January 2016, available at https://www.nytimes.com/2016/01/12/opinion/brazils-digital-backlash.html?_r=0.

[33] See, e.g., Andrew Fishman, "Brazilian Cybercrime Bills Threaten Open Internet for 200 Million People", The Intercept, April 26, 2016, available at https://theintercept.com/2016/04/26/brazilian-cybercrime-bills-threaten-open-internet-for-200-million-people/; Muggah and Thompson 2017.

[34] Souza, Steibel and Lemos, 2017, p. 16.

[35] Cit. in Iure Paiva, "National Defense Policy and the Protection of the Critical Energy Infrastructure in Brazil", Austral: Brazilian Journal of Strategy & International Relations, 5:10, 2016, pp. 173-198, p. 176.

[36] Robert Muggah and Nathan Thompson, "Brazil's Critical Infrastructure Faces a Growing Risk of Cyberattacks", CFR, April 10, 2018, available at https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks.

In addition, Brazil's National Telecommunications Agency (*Agência Nacional de Telecomunicações*, Anatel) released official **guidelines for the inspection of critical infrastructure** in 2015 and is currently reviewing cyber regulations for the telecom sector.[37] Another organization, the national electricity agency Aneel, held consultations on cyber security in 2016 to develop best practices.

While Brazil has gradually invested in building institutions to increase cyber resilience, public awareness of cyber risks is still relatively low. For instance, a report by the cyber security company Norton published in 2016 demonstrated that in Brazil 44 percent of consumers cannot identify a phishing email or have to guess if the email is legitimate and 37 percent have at least one unprotected device.[38]

2.2. Institutional landscape and key stakeholders

A complex institutional architecture has evolved at the federal and state levels addressing the growing volume and severity of cyber security threats and to conduct cyber diplomacy. Table 2 provides an overview of the key institutions and their tasks related to cyber security and internet governance.[39]

Table 2: An overview of the key institutions and stakeholders in Brazil

Institution	Description	Task(s)
GSI-PR	Advises the President on security and military affairs, including civilian aspects of cyber security and cyber defence. Relevant structures under the GSI include the Department of Information and Communication Security (DSIC-GSI), the Civil House, the Secretariat of Strategic Affairs (SAE) and the Chamber of Foreign Affairs and National Defence of the Council of the Government (CREDEN).	It proposes guidelines and strategies for cyber security through the DSIC-GSI. The future structure of the GSI-PR's cyber security and diplomacy activities will be outlined in the 2019 national cyber security strategy.
DSIC-GSI	DSIC-GSI is responsible for "guaranteeing the availability, integrity, confidentiality and authenticity of information and communication for the federal public administration". [40]	Tasks range from planning, coordinating and supervising cyber security activities within the federal government administration to formulating and implementing public information security policies and regulations. Along with the Economy Ministry, the DSIC-GSI coordinates CIIP efforts at the national level. It also shares information across network security administrators, cooperates with foreign computer incident response teams and maintains the Brazilian Computer Security and

[37] Ibid.

[38] Norton, "Norton Cyber Security Insights Report 2016", 2016, available at https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-en.pdf.

[39] For a comprehensive analysis of Brazil's institutional cyber security architecture, see Louise Hurel and Luisa Lobato, "A Strategy for Cybersecurity Governance in Brazil", Strategic Note, No 30, Rio de Janeiro: Instituto Igarapé, 2018. Also cp. Diniz, Muggah and Glenny 2014, p.19-20.

[40] Ibid, p. 19.

Institution	Description	Task(s)
		Incident Response Center (CTIR.gov).
CTIR.gov	CTIR.gov was informally set up in late 2004, formally established in May 2006 (then called General Coordination for Incident Network) and renamed in 2009 as CTIR.gov.	CTIR.gov's official mandate is to coordinate responses to cyber incidents within the federal administration. Apart from reactive actions, CTIR.gov also conducts proactive operations to prevent cyber-attacks or reduce their impact. It closely cooperates with CERT.br, federal government agencies as well as foreign CTIRs.
Civil House	The Civil House is one of the units under the Presidency.	It is tasked to oversee the concession of digital security certificates for key public infrastructure and to coordinate the ANPD.
ANPD	On 14 December 2018, outgoing President Temer issued an Executive Order that created the ANPD. It consists of five directors and will be reviewed after two years.	The ANPD oversees and enforces the LGPD. It will also assist Brazilian entities to comply with the new law.
Ministry of Defence	In the past decade, Brazil expanded its cyber defence capabilities and the role of the Ministry of Defence as well as the armed forces in cyberspace.[41]	The Ministry of Defence's 2008 National Defence Strategy and its 2012 update designated the army as the main branch responsible for cyber security, and it was also tasked to host the Cyber Defence Centre (CDCiber).
CDCiber	In 2010, the government created CDCiber to coordinate cyber defence activities. CDCiber became operational in 2012 and has since evolved as a pivotal actor in driving Brazil's cyber security policy.	Initially, its main task was to protect Brazilian networks during the 2012 UN Conference on Sustainable Development (Rio+20), and it later coordinated cyber security efforts during the 2013 World Youth Day in 2013, the 2014 World Cup and the 2016 Olympic and Paralympics Games.
Cyber Defence Command (ComDCiber)	In 2016, the Brazilian government established ComDCiber, which is an operational command group integrating members of all military branches. While it is based in the regimental structure of the army, it is run in conjunction with the Joint Staff, headed by the navy, and the Department of Management and Strategy, headed by the air force.	ComDCiber is responsible for "planning, guiding, and controlling the operative, doctrinal activities of development and preparation at the level of the Military Cyber Defence System". [42]
Brazilian Intelligence Agency (ABIN)	ABIN is responsible for protecting public institutions' networks through the development of cryptographic	These cryptographic competences are executed by the Communications Security Research and Development Centre

[41] For a comprehensive overview of the Brazilian military's cyber security governance structure, see PDCDN, Programa da Defesa Cibernetica na Defesa Nacional, 2018, available (in Portuguese) at https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/palestra_cadn_xi/xv_cadn/programa_da_defesa_cibernetica_na_defesa_nacional.pdf.

[42] Ministry of Defense, *Comando conjunto de defesa cibernética*, 2017, available at https://www.defesa.gov.br/noticias/30417-comando-conjunto-na-defesacibernetica. Quoted in Hurel and Lobato, 2018, p. 8.

Institution	Description	Task(s)
	competencies.	
Ministry of Justice	In the area of law enforcement, the Ministry of Justice and its subordinate agencies are the most pivotal actors.	The Ministry of Justice and the federal Public Prosecutor's Office are responsible for judicial aspects and the prosecution of cybercrime. The ministry also established the Cyber Crime Repression Services within the Federal Police Department (DPF) to prevent and investigate attacks against the federal government's critical infrastructure and systems.
DPF	The DPF, subordinate to the Ministry of Justice, has gradually developed capabilities to address cybercrime. It is responsible for combatting crimes against federal institutions, including cybercrime. Several DPF units are specifically devoted to cybercrime, most importantly the Unit for Combating Cybercrime (URCC), which is responsible for preventing and responding to cybercrime.	Among its competencies is the ability to start investigations of crimes against federal public institutions. The URCC is also involved in law enforcement cases and judicial cooperation both within and between countries and regions.
Ministry of Foreign Affairs (Itamaraty)	Several of the ministry's divisions address cyber security-related issues: The division of disarmament and sensitive technologies is in charge of managing various bilateral and multilateral cyber negotiations. The division of combating transnational crimes addresses cybercrime tasks with international or transnational components, including discussions on the Budapest Convention, and works closely with the Federal Police. The division for technology promotion II, part of the department of technology promotion, is in the lead of bilateral and multilateral (e.g., BRICS, ELAC, G20, Mercosor) ICT dialogues. Several divisions in the department for human rights and social affairs covered issues pertaining to digital rights.	The ministry is tasked with representing Brazil in most international negotiations on cyber security and internet governance. At the time of writing, the ministry was in the process of designating a cyber security coordinator.
Ministry of Science, Technology, Innovations and Communications (MCTIC)	This is the main ministry administering the digital transformation and connectivity projects.	In early 2018, the government published Brazil's Digital Transformation Strategy, an effort led by MCTIC to cover a broad range of issues related to the digital transformation.

Institution	Description	Task(s)
The National Telecom-munications Agency (Anatel)	Brazil's administratively and financially independent telecommunications regulatory agency was established in 1997. In 2015, Anatel released official guidelines for inspecting critical infrastructure, and has developed cyber regulations for the telecom sector subsequently. More recently, Anatel has also become increasingly active in international internet governance institutions such as the Internet Governance Forum (IGF) and Internet Corporation for Assigned Names and Numbers (ICANN).	It issues relevant norms and standards to be followed by telecommunications service providers, recognizes product certification, and represses violations to user rights. Its Superintendence of Compliance (SCO) works with the army on multisectoral critical infrastructure protection; the Superintendence of Planning and Regulating (SPR) assists public security agencies to develop telecom regulations; the International Advisory (AIN) engages in fora such as the ITU and OECD; the Technical Advisory Office (ATC) collaborates with the GSI, and the Superintendence of Spectrum and Standardization (SOR) focuses on certification.
The Brazilian Internet Steering Committee (GGI.br)	CGI.br is a multi-stakeholder organization with members from government, private sector, academia and civil society, promulgating rules for managing Brazil's internet backbone. CGI was created in May 1995 by the Ministries of Communications and Science and Technology through Interministerial Ordinance 147, amended by Presidential Decree 4,829 in September 2003, to coordinate and integrate the country's various internet service initiatives, as well as to promote services' technical quality, innovation and dissemination. It is currently composed of nine government representatives, four business representatives, four from third sector, three from the scientific and technology community, and one internet expert. The committee is chaired by the MCTIC representative.	It is tasked with managing and operating Brazil's country code top-level domain name (ccTLD), .br, and oversees domain names across Latin America. In 2009 CGI.br shifted from a narrow technical focus to also addressing broader legal issues by publishing a list of ten principles for internet governance that significantly influenced the MCI. It organized the NetMundial conference in 2014 as well as two IETF and ITF conferences, and has maintained a formal relationship with ICANN since 2007 through the latter's Accountability Framework program. More recently, it also provided analysis on broader political issues such as the role of disinformation in elections, and teaching for judges on digital electoral processes.
Brazilian Network Information Center (NIC.br)	NIC.br is a non-profit civil entity implementing CGI.br's decisions and projects.	NIC.br functions as GGI.br's executive arm.
Computer Emergency Response Team (CERT.br)	To increase resilience of Brazilian networks, CGI.br created CERT.br in June 1997.	CERT.br gradually became responsible for reporting and managing computer security incidents affecting Brazilian networks and raising awareness on security vulnerabilities. While CERT.br responds to computer security attacks against critical infrastructures, CTIR.br focused on incidents affecting the federal government and administration.
Civil society	Civil society actors form a part of Brazil's cyber policy regime also beyond the CGI.br membership, including among many others Article 19, Coding Rights, Data Privacy, the Fundação Getúlio Vargas law schools' Centre	Civil society actors play a crucial role in advocacy, monitoring, and implementation of policies, digital rights and/or standards.

Institution	Description	Task(s)
	for Technology and Society (CTS) in Rio and Research Center on Law and Technology in São Paulo as well as its departments of International Relations Department and Public Policy Analysis, IDEC, the Institute for Technology and Society of Rio de Janeiro (ITS Rio), and InternetLab.	

2.3. Main policy issues and priorities

Several domestic political issues salient to Brazil's cyber diplomacy have already been discussed with a focus on legislative and regulatory developments above, including data protection, cybercrime and resilience. The section below addresses these and other salient issues beyond their legislative and regulatory dimensions, and outlines how these will likely develop in the short to medium time period.

2.3.1. Data protection and privacy

As outlined above, data protection was a pivotal issue in recent Brazilian politics and will likely remain a highly contested political issue given that President Jair Bolsonaro, in office since January 2019, has strongly opposed the MCI.[43] The decision to link the ANPD to the Presidency has also been criticized by various observers who question the authority's independence.

The protection of personal data has received particularly high attention, including during Brazil's own general elections in 2018. Brazil has been a champion of privacy rights internationally, a role catalysed by a widely acclaimed speech on data privacy before the United Nations General Assembly (UNGA) by President Dilma Rousseff's in September 2013. More recently, concerns related to fierce anti-cybercrime measures have focused on biometrics and facial recognition technology used by Brazilian companies. "Surveillance systems" are growing across Latin America, often with the support of Chinese companies.

In addition, net neutrality has been another contentious political issue. As a response to wide-spread discontent among citizens and businesses following an announcement that internet service providers (ISPs) would impose data caps on broadband internet in March 2016, the Brazilian Senate passed a bill (PLS 174/2016) that prohibited data caps on fixed broadband in March 2017, which at the time of writing still had to be approved by the House of Representatives. Proponents of net neutrality campaigned for further regulation to prevent ISPs from exploiting data caps for commercial purposes by discriminating what data is counted against bandwidth caps.

2.3.2. Disinformation

In the run-up to Brazil's 2018 general elections, political campaigns and the public paid considerable attention to the issue of disinformation.[44] Several Brazilian institutions initiated efforts to tackle the spread of disinformation, including ten draft bills in the first four months of 2018 to criminalize the

[43] "Marco Civil da Internet Criticado por Jair Bolsonaro", n.a., available at https://www.dailymotion.com/video/x32dymr.

[44] For an insightful analysis of the use of Twitter during the 2018 elections, see Caio Machado et al., *News and Political Information Consumption in Brazil: Mapping the 2018 Brazilian Presidential Election on Twitter*, Oxford: Oxford University Internet Institute, 2018, available at https://www.cfr.org/blog/whatsapps-influence-brazilian-election-and-how-it-helped-jair-bolsonaro-win. Also cp. Conor Sanchez, "Misinformation is a Threat to Democracy in the Developing World", *Net Politics*, Council on Foreign Relations, January 29, 2019, available at https://comprop.oii.ox.ac.uk/research/brazil2018/.

spread of disinformation. Among them, Brazil's Superior Electoral Court reportedly stated that significant election meddling through disinformation could even lead to the annulation of election results.[45] Online posts containing false information about candidates were subject to removal, and in July 2018 it was reported that Facebook had removed pages and accounts that allegedly spread disinformation.[46] Moreover, Facebook reportedly removed several posts linking presidential candidate Marina Silva to corruption investigations by order of the Superior Electoral Court. However, following the elections, some inquiries on disinformation have been misused to curb the freedom of the press to censor critical voices against politicians or judges, including ones by the Supreme Court.[47]

As the Brazilian population is among the world's most active social media users and producers, and WhatsApp is one the main tools used to read political and electoral information[48], the impact of disinformation is relatively strong. Therefore, political and public discourses are likely to persist, in particular on three interrelated sub-topics: liable hate speech and the responsibility of intermediaries, electoral integrity, and the misuse of personal data.[49]

2.3.3. Cybercrime and cyber defence

As outlined above, the Brazilian government has focused on strengthening the investigative capacities to fight cybercrime of the federal and state police, and sought to improve coordination between police forces in cases of cybercrime anticipation and response. Judiciary and law enforcement agencies such as the Federal Police and the Public Prosecutors promoted several measures to enhance access to user data. These efforts were linked to increased political attention to cyber security in the context of the 2014 FIFA World Cup and the 2016 Summer Olympics. In 2015 and 2016, three judicial orders temporarily **blocked WhatsApp** to force the company's parent company, Facebook, to provide communication logs or access to encrypted communications of suspects in criminal investigations. In addition, Facebook and Google executives were detained in an attempt to increase the pressure on technology companies. The shutdowns were rescinded and the executives were released within hours or days, but the incidents demonstrated both the willingness of the judiciary and law enforcement to enforce access as well as broader antagonisms between the judiciary and law enforcement agencies on the one hand side and the technology companies on the other, driven inter alia by the former's frustrations with new cryptographic systems in products by foreign technology companies. The issue of access to communications has remained contested since then. Moreover, while other countries have introduced initiatives to recruit hackers to assist in upgrading state capabilities, Brazilian institutions are divided on the matter.[50]

As outlined in detail in the introduction, concerns over several recent bills on penalizing cybercrime have been raised. Critics fear that these initiatives significantly impinge on digital freedoms. As such, digital rights groups sent an open letter to Congress in April 2016, in which they cautioned that the

[45] Machado 2018.

[46] Freedom House, "Brazil", 2018, available at https://freedomhouse.org/report/freedom-net/2018/brazil. The company Facebook has been compelled to curb the dissemination of fake news through its platform prior to mid-term elections in the US in 2018 and parliamentary elections in India in 2019, including by using artificial intelligence to identify fake accounts.

[47] Gustavo Ribeiro, Brazil's Supreme Court censors damaging report on Chief Justice", The Brazilian Report, April 15, 2019, available at https://brazilian.report/power/2019/04/15/brazil-supreme-court-censorship-crusoe/.

[48] Cristina Tardáguila, Fabrício Benevenuto and Pablo Ortellado, "Fake News is Poisoning Brazilian Politics. WhatsApp Can Stop It", New York Times, October 17, 2019, available at https://www.nytimes.com/2018/10/17/opinion/brazil-election-fake-news-whatsapp.html.

[49] Phone Interview, senior researcher, June 11, 2019.

[50] Ibid.

proposed rules would directly impinge on citizens' right and the economic freedom of ICT companies.[51] However, this has produced only moderate changes to the commission's proposals.[52]

Finally, some observers have argued that the Brazilian state has invested disproportionately in cyber warfare and counter-terrorism capabilities at the expense of what is the primary cyber threat in Brazil: Cybercrime.[53] With the creation of CDCiber in 2012, Brazil was the first country in the region to establish a dedicated military cyber-unit.[54] These observers continue to call for a rebalancing of the state's cyber security approach. Digital rights groups and civil liberty advocates, more generally, argue that the state's resources are disproportionally devoted to the military, instead of to day-to-day law enforcement.[55] According to these groups, a securitized and militarized approach towards cyber policy has already circumcised civil liberties. To illustrate the securitization of cyberspace, they point to the expansion of Brazil's cyber security and surveillance infrastructures for the FIFA World Cup and Olympic games, which were kept in place even after the events. While Brazil's then-Justice Minister Alexandre de Moraes sought to maintain these structures, civil society groups warned that these surveillance structures could be abused in the absence of effective oversight by civilian authorities.[56] More specifically, civil society actors have been wary about ABIN's media monitoring platform *Mosaico* and the CDCIber program *Guardião*, which have allegedly been used to track users and predict events but could also potentially lead to (self-) censorship and pressures on civil rights movements.[57]

This discussion illustrates that like most emerging economies with democratic political systems, Brazil has to balance competing imperatives of security, development and openness. While perceived cyber threats have significantly driven legislative proposals allowing police and government access to data without a judicial order under certain circumstances, strong opposition by congressional representatives and digital groups has often prevented an unchecked securitization of Brazil's cyber policies.[58]

2.3.4. Multistakeholder Internet Governance

Finally, the peculiar form of multistakeholder internet governance that Brazil has developed has continued to be a main focal point of Brazil's domestic cyber policy. CGI.br's secretariat had to balance the various interests and claims among stakeholders that are or want to become members of CGI.br. The expansion of CGI.br's portfolio from a technical focus on domain name management to covering economic and security issues, as well as the political nature of the process, will continue to determine the effectiveness and values of Brazil's cyber policy landscape, and by extension also have significant impact on its cyber diplomacy.

2.4. Impediments to cyber policy-making

Across the areas of privacy rights, disinformation, cybercrime and internet governance, several factors have often commonly impeded the effective implementation of policy or legislation. Four impediments are particularly tangible: (1) a lack of coordination between the multiple state and non-state actors involved, (2) a fragmentation of their responses to the proliferation of cyber threats, (3) a

[51] See Access Now, Joint statement to Brazilian congress: Drop dangerous cybercrime bills, April 1, 2016, available at https://www.accessnow.org/joint-statement-brazil-cybercrime/.
[52] Muggah and Thompson 2016.
[53] Muggah and Thompson 2017. Also cp. Daniel Woods, "Brazil's New President and the Changing Cyber Risk Landscape", *Forbes*, November 27, 2018, available at https://www.forbes.com/sites/riskmap/2018/11/27/brazils-new-president-and-the-changing-cyber-risk-landscape/#115f3cb95453.
[54] Muggah and Thompson 2016, p.27.
[55] Ibid, p.22.
[56] Ibid; see also Muggah and Thompson 2016.
[57] Diniz, Muggah and Glenny 2014, p.15.
[58] Muggah and Thompson 2017.

lack of informed public debate and (4) unclear priorities regarding public funding in the cyber security sector. Thus far, as Brazil's cyber policies have focused on data protection and efforts to curb fake news, evolving subjects with considerable salience for cyber security such as artificial intelligence have received less high-level political attention.[59] The following section will examine Brazil's diplomatic positions on cyber security and internet governance in global multilateral as well as bilateral and regional negotiations.

3. Brazil's global, regional and bilateral cyber diplomacy

3.1. Brazil's multilateral and multistakeholder cyber diplomacy

In the past decade, international debates on **internet governance** have been split into two broad camps, with one group that traditionally advocated granting greater authority to national governments and replacing ICANN with the ITU as the main coordinating institution, and another that supported the multi-stakeholder model in line with ICANN's mandate.[60] Brazil, which has been one of the leading voices for reforming the global internet governance structure, has long been perceived as a "swing state" in these debates, reluctant to fully endorse either camp.[61] On the one hand, Brazil adopted CGI.br's ten principles that emphasized freedom, privacy and human rights in 2010 as well as the MCI in 2014, proposed a global bill of rights for internet activity (a global version of its MCI) in 2014, and recurrently called for an increase of multi-stakeholder approaches to internet governance. On the other hand, Brasilia expressed its support for the idea of an international treaty under UN supervision that would regulate the internet, for instance at the UN-sponsored World Conference on International Telecommunications (WCIT) in Dubai in 2012, a push opposed by those warning of disproportional powers of governments and the legitimation of restrictive or intrusive measures.[62]

Brazilian diplomats portray Brazil's role in the often polarized debates on internet governance or norms of responsible state behaviour as that of a broker or strategic bridge builder between the different camps rather than a swing state, and highlight that balancing between both camps serves to maintain an independent foreign policy.[63] For example, Brazilian officials reportedly sought to reconcile divergent positions between China and Russia on the one hand and the US on the other at ICANN and UNGA meetings, where they highlighted the compatibility of multilateral and multistakeholder approaches to internet governance.[64]

Following the Snowden revelations in 2013, Brazil became a prominent voice promoting privacy rights internationally and denouncing US influence over ICANN, and advocated for more inclusiveness and accountability of the global internet governance model.[65] Brazil and Germany – both strongly affected by NSA surveillance operations – led global diplomatic efforts to regulate surveillance issues. In September 2013, at the opening of the **68th Session of the UNGA**, then-President Dilma Rousseff argued that the NSA's activities violated international law, notably national sovereignty, human rights and civil liberties, and emphasized the need to develop an alternative, non-discriminatory multilateral

[59] Interview with a civil society representative, December 3, 2018.
[60] Elena Lazarou, "EU-Brazil cooperation on internet governance and ICT issues", *European Parliament,* November 2015, available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571309/ EPRS_BRI(2015)571309_EN.pdf.
[61] Tim Maurer and Robert Morgus, *Visualizing Swing States in the Global Internet Governance Debate*, Internet Governance Paper No. 7, Waterloo, Ontario: CIGI, 2014.
[62] Diniz, Muggah and Glenny 2014.
[63] Interview with senior official, Itamaraty, June 5, 2019, Brasilia, Brazil.
[64] Alex Grigsby, "The Brazil-US Cyber Relationship is Back on Track", *Council on Foreign Relations*, July 1, 2015, available at https://www.cfr.org/blog/brazil-us-cyber-relationship-back-track.
[65] Ibid.

governance framework to guarantee the protection of these rights.[66] As such, she called on states to ensure that the following five groups of rights will be protected in cyberspace:

- Freedom of expression, privacy of the individual and respect for human rights;
- open, multilateral and democratic governance, carried out with transparency by stimulating collective creativity and the participation of society, governments, and the private sector;
- universality that ensures social and human development and strives toward inclusive and non-discriminatory societies;
- cultural diversity, without the imposition of beliefs, customs and values; and
- neutrality of the network, guided only by technical and ethical criteria, rendering it inadmissible to restrict it for political, commercial, religious or any other purposes.[67]

At this UNGA session and with the support of Germany, Brazil submitted a draft for the "right to privacy in the digital age" to the Third Committee of the UNGA, which was adopted without a vote.[68] The text established for the first time that human rights would need to be equally protected offline and online. As a result, the UN Human Rights Council in April 2015 also adopted resolution 28/16 that established the three-year position of a Special Rapporteur on the right to privacy mandated to report on alleged violations of privacy rights including in connection with emerging technologies.

Drawing on its two-decade experience with domestic multistakeholder governance, Brazil has also played a pivotal role in multilateral negotiations on promoting a genuinely multistakeholder system. Subsequent to the UNGA session in 2013, ICANN CEO Fadi Chehade and President Rousseff announced that Brazil would host a **Global Multistakeholder Meeting on the Future of Internet Governance** (NETMundial) with representatives from the public and the private sector from 80 countries in 2014. The meeting in São Paulo resulted in the *NETMundial Multistakeholder Statement* that contained a shared set of non-binding principles governing the internet and roadmap for the future evolution of the internet governance system as well as recommendations for measures to transform ICANN into a "truly international and global organisation serving the public interest".[69] The statement expressed the signatories' preferences for the post-2015 development agenda, the World Summit on the Information Society (WSIS) +10 Process and ensuing IGFs.

Following the meeting, CGI.br in cooperation with ICANN and the World Economic Forum launched the *NETMundial Initiative* in 2014 to establish an open source platform providing assistance on non-technical issues such as legal questions related to domain names management. However, the initiative faded by 2016 as alleged struggles over various stakeholders' representation at the Inaugural Coordination Council as well as concerns over potential interference with the UN IGF persisted. While CGI.br sought to preserve the initiative, ICANN and WEF withdrew their financial support.[70]

---

[66] Lazarou 2015.

[67] UN, "Third Committee Approves Text Titled 'Right to Privacy in the Digital Age'. GA/SHC/4094", November 26, 2013, available at https://www.un.org/press/en/2013/gashc4094.doc.htm, See also Claudio Ruiz, "Could Brazil become the leader in Internet governance?", p. 121-122, in Eduardo Magrani (Ed.), "Digital Rights: Latin America and the Caribbean", *FGV Direito Rio*, 2017. Before the speech, President Rousseff reportedly invited the 21 CGI.br members and CGI.br's Executive Secretary to Brasilia to present CGI.br's ten principles – five out of the ten principles were selected and formed the core of Rousseff's proposal for an international bill. Interview with senior official, CGI.br, June 4, 2019, Brasilia, Brazil.

[68] Vales, 2014, p. 304.

[69] Lazarou 2015.

[70] Reportedly, ICANN's initiative to partner with WEF for the NETMundial also contributed to the initiative's failure, as WEF was widely perceived as an exclusive Western club. Interview with civil society representative, June 4, 2019. At the IGF in

Brazil has also actively engaged in efforts to reform the global internet governance architecture beyond NetMundial. For instance, Brasilia was a member of the UN ICT Task Force founded in 2001 under the UN Economic and Social Council (ECOSOC) and contributed to the definition of internet governance at the WSIS in 2005. In addition, CGI.br has representatives at the Internet Engineering Task Force (IETF) and ICANN[71], and Brazil supported international efforts to strengthening the IGF within the architecture of global internet governance, hosting its 10th meeting in João Pessoa in November 2015.

Finally, Brazilian delegations have played a significant role in voicing a Global South perspective in multilateral negotiations on international norms of responsible state behaviour. Brazil attended all sessions of the **UNGGE** except the one between 2012 and 2013. Chairing the fourth session between 2014 and 2015, it helped bridge the different positions on cyber norms and produce a concluding report that still constitutes the pivotal reference document on norms of responsible state behaviour in and the application of international law to cyberspace. It also participated in the fifth UNGGE, which however ended in a deadlock and failed to produce a consensus report. Most recently, Brazil endorsed the UNGA resolution 73/266 establishing another UNGGE, and abstained from the vote on the UNGA resolution 73/27 establishing an Open-Ended Working Group (OEWG) on the "Developments in the field of information and telecommunications in the context of international security" open to all UN member states.[72] The UNGGE held its first meeting in December 2019 in New York and will submit its final report to the UNGA in 2021 during its 76th session. It will comprise of 25 members based on equitable geographical distribution, including for the first time all members of the BRICS (Brazil, Russia, India, China, South Africa) grouping. The UNGGE chairman is also mandated to conduct consultations with regional organizations prior to the first meeting. The OEWG held its first substantive meeting in September 2019 and will report back to the UNGA during its 75th session in 2020.[73] The establishment of this dual track marked the split of the UN-level negotiations on international norms of responsible state behaviour in cyberspace.

Brazil accepted to chair the sixth UNGGE, becoming the only one of two states that chaired the group twice.[74] The government designated Ambassador Guilherme Patriota, Brazil's former Special Representative of Brazil to the Conference on Disarmament in Geneva now posted in Mumbai, as its UNGGE representative. In mid-2019, Ambassador Patriota travelled to Bratislava, Vienna and Brussels to conduct consultations with ROs including the EU. In this context, he and Brasilia-based diplomats highlighted the importance of making both processes a success and avoiding a zero-sum mind-set, an objective shared with EU member states.[75] Accordingly, Brazil seeks to use its chairmanship to focus on three issues: the role of civilians in cyber conflict and the applicability of international humanitarian

---

November 2019 in Berlin, participants will nevertheless meet on a panel titled NetMundial + 5 that reviews the last five years of progress on the principles and the roadmap.

[71] Anatel leads the Brazilian delegation at the International Telecommunications Union (ITU).

[72] "Advancing responsible State behaviour in cyberspace in the context of international security", Document A/C.1/73/L.37, *UN General Assembly,* 18 October 2018, available at http://www.un.org/ga/search/ view_doc.asp?symbol=A/C.1/73/L.37 . "Developments in the field of information and telecommunications in the context of international security", Document A/C.1/73/L.27, *UN General Assembly,* 22 October 2018, available at https://undocs.org/A/C.1/73/ L.27.

[73] UNODA, Fact Sheet. Intergovernmental Processes on the Use of Information and Telecommunications in the Context of International Security 2019-2021, 2019, available at https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf.

[74] Reportedly, the UN Secretary General offered the chairmanship to Mexico, which however had to decline given the strenuous relationship with the US and the potential frictions this constellation might have resulted in.

[75] Based on notes from informal EU-UNGGE Regional Consultations, during which the EUCD hosted Ambassador Patriota in Brussels on June 20, 2019, one day following the formal consultations, as well as on interview with senior official, Itamaraty, June 5, 2019, Brasilia, Brazil.

law, the right to respond, and attribution. However, Brazilian diplomats have expressed scepticism about the prospects for substantially advancing the UNGGE with tangible novel results, and emphasized the importance of reinforcing the results and consensus that has been achieved in previous UNGGE, including efforts to strengthen transparency and confidence building measures (TCBMs).[76]

At the first substantive session of the OEWG in September 2019, Brazil's representative reiterated that the group should focus on the development of a framework to implementing the norms, rules and principles developed in the UNGGE reports and to building capacity, and that the UN's role and capacity to address ICT-related international security challenges should be strengthened, e.g. by establishing a specialized forum focused on capacity building.[77]

Brazilian experts have also participated in the UN High-Level Panel on Digital Cooperation between 2018 and 2019 as well as the Global Commission for the Stability of Cyberspace (GCSC) inaugurated in 2017. Brazil also became the only country to twice host the annual meeting (2007 and 2015) of the Internet Governance Forum (IGF), a multistakeholder forum established by the UN in 2006.

Meanwhile, Brazil remained sceptical of other multistakeholder or private sector initiatives to help drafting norms of responsible state behaviour. For example, it declined an invitation by the French government to sign the latter's "Paris Call for Trust and Security in Cyberspace" as it was not consulted in advance. Similarly, Brazilian diplomats expressed discontent that exercises such as the Tallinn Manuals largely failed to include non-Western experts and called for making future initiatives more inclusive.[78]

Overall, successive Brazilian governments have made privacy protection, inclusiveness and stability central themes of Brazil's cyber diplomacy. Brazil has played a central role in both multilateral and multistakeholder arenas of internet governance and cyber security negotiations. Some observers argued that the focus of Brazil's engagement in international cyber debates is likely to shift toward an emphasis of cyber security under the government of President Bolsonaro.[79] Similarly, Brazilian civil society organizations are expected to increasingly reach out abroad for funding and support.[80]

3.2. Brazil's bilateral, regional and plurilateral cyber diplomacy

Beyond multilateral and multistakeholder cyber diplomacy, Brazil has sought to advance its interests through bilateral, regional and plurilateral channels. At the **bilateral level**, the defence ministers of Argentina and Brazil signed a Joint Declaration to review bilateral cooperation in the field of defence, including cyber defence, in 2011.[81] Brazil and Argentina have worked together through the Subgroup on Cooperation in Cyber Defence: according to Brazil's Ministry of Defence, the two states cooperated on information exchange, research training and exercises between 2014 and 2017.[82] Furthermore, during closed-door meetings with the Pentagon, the defence ministers of Brazil, Chile and Colombia reportedly reviewed cyber threats and asked for support to strengthen the resilience of their networks.[83] Finally, the Brazilian Ministry of Defence organized the first Cyber Defence Training for

[76] Ibid.
[77] For the video recording of the OEWG meetings, see United Nations, *Open-Ended Working Group*, 2019, available at https://www.un.org/disarmament/open-ended-working-group/
[78] Interview with senior official, Itamaraty, June 5, 2019, Brasilia, Brazil.
[79] Daniel Woods, "Brazil's New President and the Changing Cyber Risk Landscape", *Forbes*, November 27, 2018, available at https://www.forbes.com/sites/riskmap/2018/11/27/brazils-new-president-and-the-changing-cyber-risk-landscape/.
[80] Interview with a civil society representative, December 3, 2018.
[81] Diniz, Muggah and Glenny 2014, p. 28.
[82] "Brazil: Investigating policy initiatives on cyber security and cyber-defence in South America", *Article 19*.
[83] Diniz, Muggah and Glenny 2014, p. 28.

Officers of Friendly Nations in 2016, which was attended by representatives from 12 countries around the world.[84]

Brazil also entered multiple dialogues with countries beyond Latin America.[85] Brazil's relationship with the world's most potent "cyber power", the United States, has been severely impaired by a significant level of distrust.[86] In 2010, both countries' defence ministers signed the Brazil-US Defence Cooperation Agreement promoting among others cooperation on technology security. During President Rousseff's visit to the US in April 2012, both countries established the US-Brazil Defence Cooperation Dialogue, enhancing cooperation in cyber defence exercises. On this occasion, both governments also established the US-Brazil Internet and ICT Working Group, which was however disbanded after the Snowden revelations in 2013, following which President Rousseff had cancelled her planned 2013 US visit. After it became known that President Obama had not been directly involved in the surveillance programs targeting Brazil, Presidents Obama and Rousseff committed to resume the dialogue during the latter's US visit in June 2015, highlighting in a joint statement that both governments are "partners in strengthening the 'multistakeholder' approach to Internet governance to preserve the benefits of a single, reliable, open, interoperable, and secure Internet", and to improve their collaboration in consultation with multiple stakeholders on cyber security, cybercrime prevention, capacity building, and norms of responsible state behaviour in peacetime.[87]

However, Brazil's political left commonly viewed the US with resentment and suspicion, and the dialogue failed to produce major, tangible results. With the election of President Bolsonaro, who strongly committed to further improve ties with the US and review relations with China during his campaign, this foreign policy orientation is likely to change. In addition, Brazil's foreign minister under President Bolsonaro, Ernesto Araújo, served as a midlevel diplomat heading Itamaraty's US and Canada department, and shared the President's goal to align with US President Trump.[88] Already, both sides signed agreements on research, security and defence. In July 2019, US President Trump designated Brazil as a major non-NATO ally, allowing Brazil to receive preferential access to US military equipment and technology. Against this background, Brazilian-US cooperation on cyber security and internet governance can be expected to intensify, although the imposition of US metal tarrifs on Brazil announced in December 2019 could shatter previous agreements.

At the same time, Brazil has also cautiously cultivated growing cyber cooperation with Russia. Building on the gradual rapprochement between both countries in the 1990s after relations were largely dormant during the Cold War, cooperation in multilateral fora such as the G20 and BRICS and on trade and commerce, including related to military technology, intensified. In 2004, both countries established a "Technological Alliance", which was further endorsed in the strategic partnership agreement of 2005. Since then, cooperation has deepened, and while Brazil abstained from a vote against Russia in a UN resolution that condemned Russia's annexation of Crimea, Russia has supported Brazil's candidacy for a permanent UN Security Council seat. However, Brazil was careful not to subscribe unconditionally to Russian cyber diplomacy initiatives. For instance, while Brazil has supported the Russia-driven idea of a code of conduct on information weapons, signed the bilateral

[84] "Brazil: Investigating policy initiatives on cyber security and cyber-defence in South America", *Article 19*.

[85] Brazil's bilateral dialogues with EU member states will discussed in the section 4.2 below.

[86] See Harold Trinkunas and Ian Wallace, *Converging on the Future of Global Internet Governance. The United States and Brazil*, Washington, DC: Brookings Institution, 2015.

[87] White House, *FACT SHEET: The United States and Brazil - A Mature and Multi-Faceted Partnership*, June 30, 2015, available at https://obamawhitehouse.archives.gov/the-press-office/2015/06/30/fact-sheet-united-states-and-brazil-mature-and-multi-faceted-partnership.

[88] Ernesto Londoño and Shasta Darlington, "US and Brazil Chose Similar Leaders. It May Lead to Smoother Relations", *The New York Times*, November 20, 2018, available at https://www.nytimes.com/2018/11/20/world/americas/bolsonaro-brazil-trump.html?login=email&auth=login-email.

Agreement on Non-Aggression by Information Weapons with Russia to enhance information exchange, capacity building and joint cyber warfare exercises in 2010, and voted in favour of a the proposal for a resolution on Countering the Use of ICTs for Criminal Purposes initiated by the Russian government and adopted in the Third Committee of the UNGA's 73rd session in November 2018, it has distanced itself repeatedly from Russia's preferred understanding of cyber security as entailing content control, e.g. by framing the code of conduct in terms of regulating "information weapons" rather than "information security", and abstained in the vote on the Russia-backed OEWG resolution. This cautious hedging diplomacy can be expected to continue under President Bolsonaro, whose rapprochement with the US will likely be accompanied with a decreasing focus of attention on if not greater scepticism toward Russia.

Brazil's current government is pursuing a similar hedging posture in its cyber relations toward China. President Bolsonaro publicly criticized Chinese trade and investment policies during his election campaign, but sought to balance his tilt toward the US since coming into office. China has been Brazil's main trading partner since 2009, and Bolsonaro's government avoided taking sides in the Chinese-US "trade war".[89] Its decision-making on 5G will test the viability of this balancing act: while Anatel is still working on determining the rules for the 5G spectrum auction, which is expected to take place in 2020, Brazil has thus far defied US pressure to ban the Chinese company Huawei from the auction. On internet governance, Brazil and China traditionally shared an interest in reducing the US's dominance in the global internet governance regime, but Brazilian governments have been more supportive of maintaining multistakeholder mechanisms and a strong role for ICANN than Chinese governments, which insisted on a stronger role of state governments.[90]

Finally, a bilateral partnership that is likely to be strengthened under President Bolsonaro is that with Israel, a leading technological and scientific innovation hub for cyber security solutions and provider for cyber security training. Bolsonaro has committed to intensify ties with Israel, and both governments signed a Memorandum of Understanding on Cybersecurity as well as an Agreement for Cooperation in Science and Technology during his visit to Israel in March 2019.[91] Inter alia, these will likely lead to greater engagement of Israeli cyber security companies in the Brazilian market.

At the **regional level**, various reports have highlighted the relatively high vulnerability of several Latin American countries to cyber attacks and their inability to adequately respond to cyber threats, and recommended to broaden regional cooperation.[92] Latin America's most active regional organization in the field of cyber policy is the **Organization of American States** (OAS), which adopted a regional cyber security strategy, *The Inter-American Integral Strategy to Combat Threats to Cyber Security,* already in 2004. The strategy's chief objective is to help OAS member states improve their cyber security maturity by assisting in the creation of CSIRTs and the development of national cyber security strategies, raising region-wide awareness, and enhancing regional cooperation by developing a watch and warning CSIRT network among member states.[93] The strategy also established the Cyber Security Program as a part of the Inter-American Committee against Terrorism (CICTE) to "promote and

[89] Cp. Woods, 2018.

[90] Louise Hurel and Maurício Rocha, "Brazil, China and Internet Governance. Mapping Divergence and Convergence", *Journal of China and International Relations*, Special Issue 2018, pp. 98-115.

[91] Itamaraty, *Joint Declaration on the occasion of the Official Visit of President Jair Bolsonaro to Israel*, March 31, 2019, available at http://www.itamaraty.gov.br/en/press-releases/20236-joint-declaration-on-the-occasion-of-the-oficial-visit-of-president-jair-bolsonaro-to-israel-march-31-2019.

92 E.g., see Organization of American States and Inter-American Development Bank, eds. Cybersecurity: Are We Ready in Latin America and the Caribbean? 2016 Cybersecurity Report. OAS/IDB, 2016, available at https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean.

[93] OAS, "Cyber Security", 2014, available at https://www.sites.oas.org/cyber/en/pages/default.aspx.

develop cooperation among Member States to prevent, combat and eliminate terrorism".[94] In June 2018, the OAS General Assembly adopted a resolution agreeing to develop two priority voluntary cyber confidence-building measures (CBMs) recommended by CICTE and based on the UNGGE consensus reports, namely to sharing information on member states' cyber security policies and legalisation, and to nominating a national contact point at the policy level. An OAS working group on CBMs set up in 2017 continues to develop additional CBMs. In addition, the OAS partnered with Amazon Web Services to advance cyber security education, publishing a series of White Papers on cyber security and cyber risk in 2018.[95]

Between 2005 (when Brazil joined the Committee) and 2017, Brazil attended more than 20 activities related to cyber security coordinated or supported by CICTE, and hosted several conferences with relevant OAS departments to evaluate the strategy's implementation progress and update its measures.[96] The strategy was also referenced in the development of the MCI.[97] Finally, OAS is also a relevant actor for interregional cyber cooperation. For example, it cooperates with the OSCE to enhance regional CBMs in cyberspace. In March 2018, the first meeting of the OAS' working group on cooperation and CBMs in cyberspace took place in Washington DC with participation of the OSCE – the OAS is thus the second regional organization with which the OSCE collaborates on CBMs next to the ASEAN Regional Forum.

Furthermore, Brazil has actively participated in cyber security activities within the **Union of South American Nations** (*União de Nações Sul-Americanas*, UNASUR). The Defence, Justice and Interior Ministers of the twelve UNASUR member states have focused on mechanisms to improve regional cooperation regarding transnational organized crimes, including cybercrime. UNASUR established a working group on cyber defence in 2012, which adopted guidelines on regional cyber security and defence. However, according to a report by the NGO Article 19, UNASUR's activities have been largely suspended in the context of the political and economic crisis in Venezuela.[98]

The **Southern Common Market** (*Mercado Común del Sur*, MERCOSUR) has been less active in regional cyber security and diplomacy than OAS and UNASUR. In 2013, member states passed a resolution to reject US espionage. Since then, there have reportedly been no further joint initiatives.[99] Similarly, while the **Community of Latin American and Caribbean States** (*Comunidad de Estados Latinoamericanos y Caribeños,* CELAC) was promoted as an alternative regional organization that did not include US membership, in contrast to for instance the OAS, Brazil alongside Colombia, Mexico and Costa Rica, has not shared this view.[100]

Finally, Brazil has also engaged in several multilateral networks to advance its interests in cyberspace. **BRICS**, an exclusive club of five emerging economies, has made cyber security an important component of its regular meetings. The five BRICS member states have faced similar challenges in managing the rapid digitization of their economic, political and societal systems, and shared a principled opposition to an overwhelming US dominance of the global internet governance

[94] "Inter-American Committee against Terrorism", OAS, n.d., available at http://www.oas.org/en/sms/cicte/ default.asp. For a recent evaluation of the strategy, see Organization of American States and Inter-American Development Bank, 2016.

[95] E.g., see OAS, *Managing National. Cyber Risk*, White Paper Series, Issue 2, 2018, available at https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

[96] "Brazil: Investigating policy initiatives on cyber security and cyber-defence in South America", *Article 19*, December 15, 2017, available at https://www.article19.org/resources/brazil-new-report-analyses-brazils-policy-initiatives-cybersecurity-cyber-defence-south-america/.

[97] Diniz, Muggah and Glenny 2014, p. 28.

[98] "Brazil: Investigating policy initiatives on cyber security and cyber-defence in South America", *Article 19.*

[99] Ibid.

[100] Daniela Segovia, "Latin America and the Caribbean: Between the OAS and CELAC", *European Review of Latin American and Caribbean Studies,* 95, pp. 97-107, 2013.

architecture. Cyber security was first listed in the 2013 Summit Declaration after the Snowden revelations had catalysed the political will to coordinate the BRICS member states' cyber security policies. However, a split between positions advanced by Brazil, India and South Africa on the one hand and China and Russia on the other persisted, and to date there has not been a joint BRICS proposal either on a novel internet governance body or on the code of conduct on cyber security.[101] Against this background, Brazil has sought to harness its membership in the club to increase cyber security cooperation with China and Russia without openly compromising the national principles governing its cyberspace identified in 2009.

More recently, Brazil chose to focus on cyber diplomacy-related issues in two of the four priorities of its 2019 BRICS chairmanship: one on strengthening BRICS cooperation in science, technology and innovation, and another on enhancing BRICS cooperation on the digital economy. Activities throughout the chairmanship included the BRICS Working Group Meeting on High Performance Computing and IT in May, the 5th BRICS Science, Technology and Innovation Funding Working Group Meeting and the Working Group Meeting on Security on the Usage of ICTs in August, as well as subgroups of the BRICS Think Tank Council and BRICS Academic Forum in September and the Summit itself in November. Whether these meetings will yield substantive results in the medium term will illustrate the degree of the group's convergence on cyber security. Similarly, the UNGGE negotiations will be a litmus test for the convergence of their interests related to international cyber norms, as for the first time all BRICS member states are members of the UNGGE.

4. Priorities and strategy for engagement

4.1. EU priorities and cooperation with Brazil

Brazil is one of the EU's strategic partners. In 1992, both sides formalized their ties by signing a Framework Cooperation Agreement. Subsequently, Brazil supported closer ties between the EU and MERCOSUR, facilitating the signing of a Framework Cooperation Agreement between both institutions in 1995. Since then, both sides have established several political dialogues, signed political agreements and engaged in various expert meetings and summits, with a focus on trade and commerce.[102] In 2007, the EU recognized Brazil as a key global partner by establishing the EU-Brazil Strategic Partnership, which outlines ways to enhance cooperation on climate change, sustainable energy, poverty reduction, the MERCOSUR integration process, and stability and prosperity in Latin America. This marked a turning point, as one observer noted: "After a period of relational indifference, followed by decades of minimal cooperation largely restricted to trade and economic issues, EU–Brazil relations entered a new phase with the establishment of a formal SP [Strategic Partnership] in 2007. This bilateral achievement was the corollary of the EU's partnership policy towards Brazil, which, for more than a decade, was mainly governed by the 1992 EC–Brazil Framework Cooperation Agreement and the 1995 EU– MERCOSUR Framework Cooperation Agreement."[103] Several sectoral political dialogues on issues ranging from climate change and organized crime to terrorism as well as two Joint

[101] Hannes Ebert and Tim Maurer, "Cyberspace and the Rise of the BRICS", *Journal of International Affairs*, October 12, 2013, available at https://jia.sipa.columbia.edu/online-articles/cyberspace-and-rise-brics. In fact, the three democracies had coordinated their global internet governance policies in a separate institution, the India-Brazil-South Africa Forum (IBSA), since its creation in 2003.

[102] For an overview of the bilateral relations, see Eleonora Poli, External Actions in a Multilateral Arena: An Analysis of EU Relations with Brazil, IAI Papers 18, July 2018, Rome: IAI.

[103] Laura Ferreira-Pereira, "The European Union's partnership policy towards Brazil: more than meets the eye", *Cambridge Review of International Affairs*, 29:1, pp. 55-77, 2016, p. 73.

Action Plans were established to operationalize the Strategic Partnership Agreement.[104] The agreement also identified mechanisms to revitalize the cooperation between the EU and MERCOSUR, and Brazil has played an instrumental role in the ongoing discussions on an Association Agreement, including a free trade area that has been negotiated since 2000 and if ratified would constitute the largest of its kind.

Yet, the implementation of the Strategic Partnership Agreement objectives was derailed by the 2008-9 global financial and economic crisis. Both sides were preoccupied with handling the crisis' repercussions. In addition, Brazilian diplomacy also focused increasingly on South-South cooperation in institutions such the BRIC (and later BRICS), BASIC (Brazil, South Africa, India, China), and IBSA (India, Brazil, South Africa) groupings. In 2016, driven by multiple instabilities within Europe as well as its neighbouring regions, China's ascendance, and the rise of several new powers, the EU published the EU Global Strategy (EUGS), in which it also pledged to revitalize its cooperation and strategic partnerships with regional powers to sustain a rules-based international order. In 2017, while the EU was Brazil's second-biggest trading partner, Brazil was only the EU's eleventh biggest, and most observers acknowledged that enhanced cooperation would be mutually beneficial.[105] While the EUGS did not refer to Brazil or Latin America specifically, it paved the way for new initiatives, including in the area of science and technology. In fact, the European Commission recently noted that the "(t)he EU's cooperation with Brazil on Science & Technology is one of the most active areas in the Strategic Partnership".[106] Expectations regarding technology cooperation were high in the drafting of the Strategic Partnership, as it was expected that it would create the necessary conditions to enhance the transfer of technology know-how from Europe to Brazil.[107] In 2017, the Strategic Partnership was renewed for another five years. While cyber cooperation focused on trade and investment issues such as digital market regulations and infrastructure development, it also encompassed strategic aspects of cyber diplomacy, as will be demonstrated in the following part.

4.2. Brazil-EU relations in cyber security and governance

Brazil and the EU established the EU-Brazil Information Society Dialogue (or ICT Dialogue) in 2010 and the EU-Brazil Cyber Dialogue in 2017. Discussions in these two tracks addressed questions related to cooperation on ICTs and research, internet governance, cybercrime and cyber norms.

4.2.1. ICT and research

Within the framework of the Strategic Partnership, Brazil and the EU have engaged in the bilateral Information Society Dialogue (or ICT Dialogue) to enhance cooperation on policies, regulations and standards, and research cooperation in the ICT sector since 2010. The dialogue meetings are led by DG Connect on the EU side and MCTIC on the Brazilian side, and take place on an annual base. During the EU-Brazil Information Society Dialogue in 2012, the two delegations "shared their experience and knowledge of policy and regulatory issues in areas such as broadband development, governance and internet security, cloud computing and digital content".[108] During the 2016 EU-Brazil ICT Dialogue, discussions focused on the EU's Digital Market Strategy and data protection laws (the Marco Civil and GDPR), as well as on connectivity. The Commission highlighted the "Gigabit Society" initiative to

[104] By 2016, regular dialogues had been set up in over 15 areas, see Delegation of the EU to Brazil, *Brazil and the EU*, 2016, available at https://eeas.europa.eu/delegations/brazil_en/986/Brazil%20and%20the%20EU.

[105] European Commission, *Countries and regions. Brazil*, 2019, available at http://ec.europa.eu/trade/policy/countries-and-regions/countries/brazil/.

[106] European Commission, *Digital Single Market. Americas*, 2019, available at https://ec.europa.eu/digital-single-market/en/americas.

[107] Laura Ferreira-Pereira, 2016, p. 76.

[108] EEAS, "Brazil and the EU", 2016, available at https://eeas.europa.eu/delegations/brazil_en/986/ Brazil%20and%20the%20EU.

enhance connectivity within the EU. Anatel and the Commission agreed to maintain the exchange on connectivity issues and, for instance, the role of competition policy in this field.[109]

The Commission also highlighted "the work on open platforms and especially FIWARE, where the Brazilian universities, municipalities and various companies including start-ups are exploring the potential of open platforms for the developments of applications for smart / digital cities which is resulting in the emergence of a FIWARE-based eco-system" as an example of successful cooperation.[110] In this regard, the two actors started linking StartUpEurope and Start-up Brazil, comparable to "the partnership that EU is developing with other start up ecosystems in Silicon Valley, and India".[111] Finally, on the 10th edition in December 2017, discussions went beyond the traditional focus on research and innovation and emphasized the need to cooperate on policy-making for digital transformation.[112] While the 2018 dialogue was skipped as a result of the 2018 elections in Brazil, it was resumed in November 2019.

As one of the major outcomes of the dialogue, the two sides at the EU-Brazil Summit in 2014 decided to build an optical submarine fiber-cable (EllaLink) to connect Brazil (and subsequently South America) and the EU (Portugal) to increase the autonomy of their data flows. In 2015, 80-85 per cent of all digital traffic between Latin America and Europe was routed through the United States.[113] The Brazilian telecom provider Telebras and Spanish cable operator Islalink were tasked to construct the cable between Fortaleza and Lisbon.[114] Telebras reportedly argued that the project would make interregional connection more secure and less prone to espionage.[115] The EU invested €25 million through the acquisition of capacity for research and education networks (e-infrastructures). At the time of writing, the cable was expected to be operational in 2020.[116]

Moreover, the volume of Brazil-EU joint cyber-related research has grown significantly over the past decade. In 2004, both sides signed the Agreement for Scientific and Technological (S&T) Cooperation, which entered into force in 2007 and has governed the bilateral cooperation on research and innovation since. The Agreement was "intended to encourage, develop and facilitate cooperative activities in areas of common interest and is based on the principles of mutual benefit, timely exchange of information, reciprocal access to activities undertaken by each Party and appropriate protection of intellectual property rights."[117] Since it entered into force, over 350 joint projects in the field of research and innovation have been pursued, many of which focused on ICT-related issues ranging from broadband development, cloud computing, digital broadcasting and 5G to internet governance and technology regulation.[118] Funding of related joint activities in successive joint calls aligned with the EU's Seventh Framework Programme (FP7) and Horizon 2020 programme amounted to an overall investment of around €50 million.

---

[109] "Working together with Brazil on digital issues", European Commission, 18 November 2016, available at https://ec.europa.eu/digital-single-market/en/blog/working-together-brazil-digital-issues.

[110] Ibid.

[111] Ibid.

[112] European Commission 2019.

[113] Lazarou 2015.

[114] For details on the BELLA project (Building the Europe Link with Latin America), see European Commission, "BELLA: A new digital data highway between Europe and Latin America, available at https://ec.europa.eu/digital-single-market/en/news/bella-new-digital-data-highway-between-europe-and-latin-america.

[115] "Brasil assina acordo de construção de novo cabo submarino de internet com a Europa", *Exame*, July 1, 2015, available (in Portuguese) at https://exame.abril.com.br/tecnologia/cabo-submarino-de-comunicacao-vai-ligar-fortaleza-a-lisboa-em-2017-2018/.

[116] "Express Subsea Cable System between Europe & Latin America" *EllaLink,* 2019, available at https://ella.link/.

[117] European Commission, Roadmap for EU-Brazil STI cooperation, October 2018, p. 1.

[118] European Commission, "New mechanisms to support EU – Brazil cooperation in research and innovation", *European Commission,* 22 May 2018, available at http://ec.europa.eu/research/iscp/index.cfm?pg=brazil.

At the Mobile World Congress in February 2016, Brazil and the EU also signed an agreement to develop 5G. According to the agreement, the two partners will:

- Develop a global definition of 5G and identify the services that should be the first delivered by 5G networks;
- work to define common standards in order to have a stronger position on the global stage;
- cooperate in identifying the most promising radio frequencies to meet the additional spectrum requirements for 5G; and
- promote the deployment of 5G in fields like smart cities, agro-food, education, health, transport or energy as well as possibilities for joint research projects in this area.[119]

Following this agreement, the European Commission, the Brazilian government, the 5G Infrastructure Association representing the leading European 5G research initiative, and the Brazilian 5G initiative Telebrasil – Projeto 5G signed a Memorandum of Understanding to foster industrial collaboration on 5G development in March 2017.[120] Brazil and the EU also opened the ICT week in Brasilia in December 2017, discussing 5G, IoT, artificial intelligence and advanced manufacturing.[121]

In May 2018, the European Commission, the Brazilian National Council for Scientific and Technological Development, the Brazilian Funding Agency for Studies and Projects and the Brazilian National Council of State Funding Agencies signed an arrangement enabling "co-funding of Brazilian participation in Horizon 2020 [...] extending to the entire country". Previously, co-funding was only available in eight Brazilian states. The arrangement also describes "necessary operational steps for launching coordinated calls and for twinning of project areas in common interest". [122]

More recently, at the Brazil-EU Digital Economy Dialogue in Brussels in December 2019, Brazil and the EU committed to align methods and standards on equipment certification in the context of 5G security, a point that had been put on the agenda during the 10th dialogue meeting.[123] Certification constituted a key priority in the EU's Cybersecurity Act, which entered into force in June 2019 and established an EU-wide certification framework for ICT digital products, services and processes. Both sides agreed to discuss certification in the context of 5G security during another meeting in 2020.

4.2.2. Internet Governance

Driven to a significant degree by the Snowden revelations, Brazil and the EU have also agreed on the need to support inclusive and transparent internet governance based on a multistakeholder governance model.[124] In the Joint Report of the Seventh EU-Brazil Summit in February 2014, Brazil and the EU agreed to establish the EU-Brazil Dialogue on International Cyber Policy (or EU-Brazil Cyber Dialogue) as part of the Strategic Partnership. The proposal was translated into concrete initiatives in the EU-Brazil Joint Action Plan 2015-2017. Also in February 2014, the European

[119] "EU and Brazil to work together on 5G mobile technology", *European Commission,* 23 February 2016, available at http://europa.eu/rapid/press-release_IP-16-382_en.htm.

[120] "The 5G Infrastructure Association and the Telebrasil – Projeto 5G Brazil sign a Memorandum of Understanding to foster industrial collaboration on Research, Standards, Regulations and Policies over the next 3 years", 1 March 2017, available at https://5g-ppp.eu/wp-content/uploads/2017/01/5G-IA-TeleBrasil-MoU-Press-Release-_-MWC2017.pdf.

[121] The first edition of the ICT week took place in 2016. For details, see "Innovation and digital transformation are the main focus of ICT Week 2017", 5 December 2017, available at http://sectordialogues.org/news/innovation-and-digital-transformation-are-the-main-focus-of-ict-week-2017.

[122] European Commission 2018.

[123] European Commision, "11th EU-Brazil Digital Economy Dialogue – Joint statement", 20 December 2019, available at https://ec.europa.eu/digital-single-market/en/news/11th-eu-brazil-digital-economy-dialogue-joint-statement.

[124] Lazarou 2015.

Commission called for more "transparent, accountable and inclusive (internet) governance".[125] In March 2014, the European Parliament adopted a resolution calling on member states to support the resolution on "the right to privacy in the digital age" initiated by Brazil and Germany and adopted by the UNGA in November 2013 and to take "further action for the defence of the fundamental right to privacy and data protection at an international level while avoiding any facilitation of state control or censorship or the fragmentation of the internet".[126] At an ICANN High-Level Group meeting in London in June 2014, the European Commission also expressed support for the results of NETMundial and its principles of inclusiveness, legitimacy, accountability, global public interest, rule of law and the separation of policy and technical functions, as well as more generally a multistakeholder model for internet governance that entails a strong role for ICANN and the IGF.[127] In its November 2014 *Conclusions on Internet Governance*, the Council sought to diffuse these principles across the EU and invited the Commission and the member states to endorse and promote the principles and multi-stakeholder internet governance.[128]

Since then, cooperation on internet governance issues intensified, including at the bilateral level. Most importantly, Brazil joined forces with Germany, with which it introduced six resolutions on the right to privacy at the UNGA and the UN Human Rights Council since 2013.[129] Brazil has been identified by observers as one of 30 "top swing states" in global internet governance debates, i.e. a state "whose mixed political orientation gives it a greater impact than its population or economic output might warrant and that has the resources that enable it to decisively influence the trajectory of an international process".[130] As a swing state with considerable diplomatic clout in the region and in global governance institutions, Brazil thus constitutes a critical partner for the EU's positioning in multilateral internet governance negotiations.[131]

4.2.3. Cybercrime

Brazil and the EU recognized the growing threat from cybercrime and destabilizing implications of vulnerable Brazilian networks and jointly addressed this threat. On 11 April 2017, the Brazilian Federal Police (BFP) and Europol signed a strategic cooperation to "combat cross-border criminal activities" including cybercrime.[132]

However, as outlined above, Brazil until recently has been reluctant to cooperate with the EU in the framework of the Budapest Convention. While Brazilian diplomats have portrayed the Brazilian role as one of a bridge builder between the proponents and the opponents of the convention, successive governments have alleged that non-members of the Council were deliberately excluded from the convention's drafting process and its regulations are biased in favour of members. Therefore, Brasilia sought to strengthen alternative multilateral institutions to address cybercrime, and recurrently

[125] European Commission, "Commission to pursue role as honest broker in future global negotiations on Internet Governance", *Press Release*, February 12, 2014, available at http://europa.eu/rapid/press-release_IP-14-142_en.htm.

[126] European Parliament, *EP resolution 2013/2188 (INI) on the US NSA surveillance programme*, March 12, 2014, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230.

[127] European Commission, "What next for Internet Governance after NETmundial?", Press Release, June 23, 2014, http://europa.eu/rapid/press-release_SPEECH-14-496_en.htm.

[128] Council of the European Union, Council conclusions on Internet Governance, November 27, 2014, available at http://italia2014.eu/media/3769/council-conclusions-on-internet-governance.pdf.

[129] German Federal Foreign Ministry, *Speech by Foreign Minister Heiko Maas at the opening of the FUTURE AFFAIRS Conference*, May 29, 2019, available at https://www.auswaertiges-amt.de/en/newsroom/news/maas-future-affairs/2222698.

[130] Maurer and Morgus, 2014, p. 4.

[131] See Thomas Renard, "EU cyber partnerships", p. 14.

[132] Europol, "Today, Brazil and Europol signed an agreement to expand cooperation to combat cross-border criminal activities", April 11, 2017, available at https://www.europol.europa.eu/newsroom/news/today-brazil-and-europol-signed-agreement-to-expand-cooperation-to-combat-cross-border-criminal-activities.

referred to the work of the open-ended Intergovernmental Expert Group on Cybercrime at UNODC.[133] Brazil committed to draft an international convention on cybercrime together with the UNODC and other South American states at the 12th UN Congress on Crime Prevention and Criminal Justice in Salvador in 2010. However, this process was derailed since then. In 2013, Brazil again supported a UN proposal by China and Russia to draft a new cybercrime treaty and strengthen the UN's Crime Prevention and Criminal Justice Programme, contradicting the EU's preference to promoting existing international legal instruments such as the Budapest Convention.

Similarly, Brazil in contrast to most European states but alongside other democracies such as India, Nigeria and Singapore, voted in favour of a resolution on cyber crime advanced by Russia with support from China and adopted by the UN General Assembly in November 2018 by a vote of 94 to 59 with 33 abstentions. The resolution was perceived as advancing an internet governance model that facilitates content censorship and government regulation.[134] A year later, Brazil again sided with Russia and China voting in favor of another Russia-backed resolution on cybercrime, which passed in the UN General Assembly 88-58 with 34 abstentions.[135] Brazil previously endorsed Russia's efforts to build a novel regulatory binding instrument to combat cybercrime in meetings of the BRICS leaders.[136]

4.2.4. Norms on responsible state behaviour and international law

Both Brazil and the EU have consistently agreed that international law applies to cyberspace. Brazil's role as chair of the 2015 UNGGE was recognized by European counterparts, and its successor Germany sought to build on its progress, a continuation of both states' joint efforts to promote data privacy internationally. Brazilian and European experts have also collaborated in non-governmental cyber norms building efforts such as the GCSC.

In addition, both sides agree on the importance of information sharing and the implementation of agreed upon norms, including through capacity building and CBMs, as illustrated in their statements at the first substantive OEWG meeting in September 2019.

Divergences persist over how international law applies, in particular norms applicable to wartime situations. While both Brazil and the EU expressed the view that IHL applies to cyber operations, e.g. in statements at the OEWG meeting in September 2019, Brazilian delegations recurrently expressed the concern that unqualified transfers of international humanitarian law and an unlimited right of self-defence could be construed as a pretext to unnecessarily forfeit the protective value of sovereignty and cement the status quo of US and European dominance in cyberspace, and to legitimize cyber operations during armed conflict.

[133] Interview with senior cybercrime official, Itamaraty, June 5, 2019, Brasilia, Brazil.

[134] Justin Sherman and Robert Morgus, "Breaking Down the Vote on Russia's New Cybercrime Resolution at the UN", New America, November 19, 2018, available at https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/

[135] Justin Sherman and Mark Raymond, "The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom", Washington Post, December 4, 2019, available at https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/.

[136] See, e.g., David Ignatius, "Russia is pushing to control cyberspace. We should all be worried", Washington Post, October 24, 2017, available at https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014bcc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html.

5. Conclusion

This study outlined the evolution of Brazil's legislative, institutional and strategic cyber landscape, the preferences and limits of its bilateral, regional, plurilateral and multilateral cyber diplomacy, and the promises and perils of cooperation between Brazil and the EU on ICT and research, internet governance, cybercrime and cyber norms. It found that at the domestic level, Brazil's initial advances in pioneering a benchmark for digital rights to govern its digital transformation became increasingly contested. The more state and non-state actors exploited cyberspace for commercial and political gains, the more the state felt compelled to introduce controls over digital spaces, in particular in the context of public events such as the 2014 FIFA World Cup, the 2016 Summer Olympics and the 2018 general elections. Networks of officials and civil society actors continued to defend digital rights, at times in collaboration with the private sector, yet issues of internet freedom, data protection and net neutrality became highly politicized. At the international level, Brazil championed a more decentralized global internet governance regime as well as digital rights and cyber norms at global institutions such as the IGF and the UNGGE respectively, and engaged bilaterally, regionally and globally with multiple partners to increase the resilience of its networks. In this versatile cyber diplomacy, the EU played a significant role, as both sides institutionalized their dialogue in two tracks.

Joint Brazilian-European efforts to building an open, free, and secure cyberspace are confronted with the recent rise of increased digital surveillance and repression, a growing reluctance to promote regional integration and liberal values in Europe and Latin America, as well as a global norms-building process that has become highly fragmented across private and public sectors. Yet, amidst growing geopolitical tensions between the two leading cyber powers China and the US, the Brazilian and European governments will likely be compelled to play an even greater role in reaching compromises in multilateral negotiations and furthering national and regional efforts to securing their networks.

Against this background, joint Brazilian-European efforts will benefit from sustaining and, where possible, broadening and widening their existing bilateral and multilateral dialogues. First, regularly exchanging information and best practices will build trust and ensure an up-to-date mutual understanding of both sides' assessments of threats and policy responses. Second, an enhanced dialogue can be used to coordinate both sides' efforts to more effectively draft and implement cyber norms. Brazil and the EU can build on a track record of jointly championing privacy rights internationally and advancing norms of responsible state behaviour. Recent statements by EU member states such as the Netherlands and France, who publicly outlined their positions on how international law applies to cyberspace in July and September 2019 respectively, can increase transparency in future Brazil-EU discussions on cyber norms. Third, an enhanced cyber dialogue will serve to identify the potential for coordinating diplomatic measures for preventing, detecting and responding to malicious cyber activities, ranging from technical cooperation to joint sanctions and attribution. It can also serve to develop strategies of how to jointly bridge the divides in global internet governance debates. Finally, an enhanced cyber dialogue, embedded in the broader strategic partnership, can function as a hub for exchanging expertise on and preparing joint efforts for building cyber capacity in Europe and Brazil as well as in third countries. This enhanced dialogue on cyber resilience and diplomacy will require more strategically involving Brazil's and Europe's non-governmental experts from academia, civil society, private sector and the technical community, whose diverse perspectives will provide an edge to compete in the struggles over a rules-based, inclusive and stable cyber order.

About EU CyberDirect

The **EU Cyber Direct** project supports EU cyber diplomacy efforts and consequently contributes to the development of a secure, stable and rules-based international order in cyberspace through extensive dialogues with strategic partner countries and regional/international organisations. The **EU Cyber Direct** is funded by the European Commission under the Partnership Instrument, International Digital Cooperation project: Trust and Security in Cyberspace.

DIGITAL DIALOGUES

are a series of research papers providing an overview of selected issues, policies and institutions of the EU's main strategic partners.

EU CYBER DIRECT

This project is funded by the European Union.