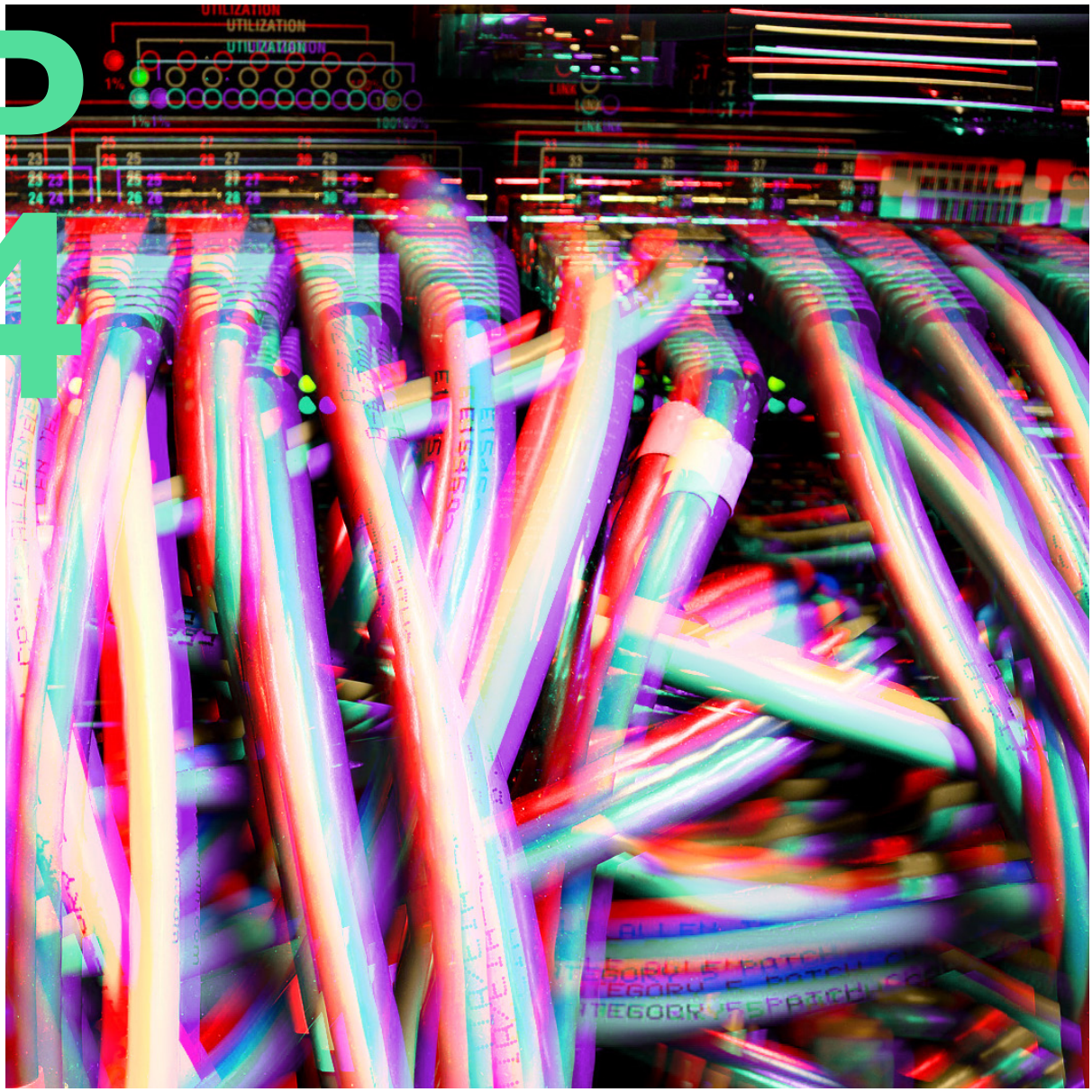
IGARAPÉ INSTITUTE
a think and do tank

SP 54



STRATEGIC PAPER

APRIL 2021

CYBERSECURITY IN BRAZIL: an analysis of the National Strategy

Louise Marie Hurel

Index

Cover photo: ElasticComputeFarm da Pixabay

CYBERSECURITY IN BRAZIL: an analysis of the National Strategy

Louise Marie Hurel

Executive Summary

In February 2020, the Decree 10.222 established Brazil's National Cybersecurity Strategy (E-Ciber) — the first official document to provide an overview regarding Brazil's role in cybersecurity, as well as objectives and guiding principles for its development between 2020 and 2023.

With the Covid-19 pandemic, thousands of people, governmental agencies, and businesses have rapidly adapted their activities to a largely virtual environment. This sudden migration led to new threats and attack surfaces for exploiting vulnerabilities. More than ever, different sectors must be prepared and trained to respond to and resist these threats. However, this was precisely the period in which Brazil suffered the worst cyber attack in its history – highlighting, yet again, that many challenges remain for ensuring that concerns with security turn into action across different sectors.

This strategic paper identifies the main gaps and challenges for cybersecurity governance in Brazil. We unpack the main elements of E-Ciber in order to understand and place the country's strategic vision historically as well as in relation to other international experiences. We adopt a principles-based approach that seeks to strengthen and inform the implementation of strategic cybersecurity objectives in Brazil, which include: national and international coordination and cooperation; knowledge integration; sustainability of efforts; and cybersecurity-related training.

This document is the result of three months of interviews with specialists from various sectors, thematic document analysis, and ethnographic work in different areas, forums, and debates.

Challenges identified in interviews and field work include:[1]

(i) The absence of a shared vocabulary when referring to cybersecurity/digital issues in society;

(ii) The association of cybersecurity with military affairs, responsibilities and institutions;

(iii) Lack of understanding regarding specific and shared digital risks across sectors;

(iv) The absence of mechanisms for sharing information regarding security risks/threats and knowledge across sectors;

(v) Lack of normative, strategic, and operational alignment for incident response; and

(vi) (vi)The existence of various cybersecurity maturity levels throughout society.

1 See Annex 1 for greater detail on the various challenges.

Acronyms

Anatel – National Telecommunications Agency BACEN –Central Bank of Brazil

CBC – Brazilian Communications Commission

CBMs – Confidence-Building Measures

CDCiber – Cyber Defense Center

CERT.br – Brazilian National Computer Emergency Response Team

ComDCiber – Cyber Defense Command

CTIR Gov –Brazilian Government Computer Security Incident Response Team

DSI / GSI-PR – Department of Information Security of the Institutional Security Office

E-Ciber – National Cybersecurity Strategy

EnaDCiber – National School of Cyber Defense

ENSIC – National Strategy for the Safety of Critical Infrastructure

GSI-PR - Institutional Security Office of the Presidency

MRE – Ministry of Foreign Affairs

OAS – Organization of American States

PNSIC – National Policy for the Security of Critical Infrastructure

REMJA - Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas

SISBIN – Brazilian Intelligence System

SMDC – Military System of Cyber Defense

UNGGE – United Nations Group of Governmental Experts

Introduction

The security of data, systems, networks, and digital infrastructures is an important dimension of an increasingly connected society. Every day, thousands of attacks are carried out on globally distributed networks, compromising businesses, services, and devices, and exposing personal and sensitive data. All of this occurs in an environment where half of the global population is connected to the internet, and where a large percentage of their online experiences are concentrated in smartphones. In Brazil alone, 70% of individuals are connected to the Internet, and 85% from classes D and E access it through their cell phones and limited data plans.[2] The question that must be considered is: how Brazil responded to national cybersecurity challenges? Brazil ranks 70th in the world on the International Telecommunications Union's Global Cybersecurity Index[3] and 6thin the Americas—behind Uruguay, Mexico, and Paraguay.

Since 2015, Brazil has been experiencing a deepening social and economic crisis, with some specialists declaring it another "lost decade"[4] for Latin America's largest country. These crises were accompanied by political and ideological challenges which signaled a troubled future for Brazil - one now worsened by the Covid-19 pandemic.

Brazil ranks 70th in the world on the International Telecommunications Union's Global Cybersecurity Index and 6th in the Americas - behind Uruguay, Mexico, and Paraguay.

In this context, Brazil and other countries in the region have found themselves more dependent on systems, networks, and Internet in order to guarantee transactions, services, and dialogue across society. Moreover, the pandemic has exposed both our dependence on the digital environment as well as the inequalities in accessibility and the lack of investment in cybersecurity (especially in the public sector).

According to the World Economic Forum Global Risks Report 2020[5] **cyber attacks and compromised information infrastructures are among the 10 greatest global risks in terms of impact.** These risks increased considerably due to the pandemic. Covid-19 not only resulted in the accelerated digitalization of businesses and services,[6, 7] but also in the creation of new attack surfaces and vulnerabilities. The increase in remote work and/or a lack of knowledge regarding good security practices can end up creating vulnerabilities in public and private sector systems, exposing them to new kinds of

2 SOPRANA, P. 70 milhões de brasileiros têm acesso precário à internet na pandemia do coronavírus. **Folha de São Paulo**. 2020. Available at: https://www1.folha.uol.com.br/mercado/2020/05/cerca-de-70-milhoes-no-brasil-tem-acesso-precario-a-internet-na-pandemia.shtml.

3 2018 Global Cybersecurity Index (GCI). **International Telecommunications Union**. 2018. Available at: https://www.itu.int/dms pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

4 STOTT, M. Latin America faces a second 'lost decade'. **Financial Times**. 2019. Available at: https://www.ft.com/content/07f0e09e--0795-11ea-9afa-d9e2401fa7ca.

5 WEF. Global Risks Report. **World Economic Forum.** 2020

6 This includes the proliferation of services rendered through applications and the expansion of the gig economy workforce- which is based on informal work mediated through digital platforms. Drastic changes in the economy during the pandemic resulted in the expanded concentration of informal work via platform. According to many already-mentioned studies, the expansion of the gig economy has disproportionately affected the middle and lower classes (De Stefano, 2016; van Doorn, 2017). In Brazil, the "Brake the Apps" protests in July 2020 were an important moment in which delivery people from different apps and different states joined together to demand a base salary for the service (Ribeiro, 2020).

7 RIBEIRO, C. Breque dos Apps: entregadores paralisam atividades novamente e fazem atos no país. **Agência Brasil.** 2020. Available at: https://agenciabrasil.ebc.com.br/radioagencia-nacional/acervo/geral/audio/2020-07/breque-dos-apps-entregadores-paralisam-atividades-novamente-e--fazem-atos-no-pais/.

attacks. Such was the case of the attack on the Superior Court of Brazil (TSJ) in November 2020. Labelled as "the worst cyber attack in the country's history"[8] , the ransomware encrypted all of the files in the judicial system's second most important court, once more demonstrating the systems' failures and the Federal Public Administration's lack of preparation in responding to these attacks.

New communications and information technology must be sustainably integrated in society. To this end, it becomes **imperative to assure not only its full capacity to function, but also the understanding of the varied risks and impacts these technologies present in exercising civil rights, in the functioning of the economy, in critical infrastructures, and in individuals' capacities to rely on these infrastructure.** As pointed out in the Digital Transformation Strategy published in 2018, the trust in the digital environment is directly related to the State's actions in the protection of rights and privacy, as well as in national security and defense.[9]

Ensuring a nation-wide digital security and cybersecurity depends on multiple actors: businesses, governments, academics, and members of civil society and the technical community. Each actor plays an important role in improving, maintaining, and constructing a resilient society that is prepared to respond to the growing security challenges. These responses range from training programs for civil society groups and investigative journalists to the elaboration of bills such as the Brazilian Data Protection Law and strategic documents such as the National Cybersecurity Strategy (E-Ciber) released in February 2020.

According to the Global Partners Digital's report on multistakeholder approaches to developing national cybersecurity strategies,[10] not all actors and sectors need to be consistently involved in all the dimensions of the governmental process of consolidating capacities and policies, **but all integrate a spectrum of expertise and play an important role in advancing public sector awareness of the different dimensions of cybersecurity -** that range from the protection of critical infrastructure, incident management, the mobilization of various forms of expertise in cyber attribution processes[11] to the preservation of human rights in policy development and implementation. In this way, each sector has an important role in not only building the country's strategic vision but also transforming it into concrete actions. They occupy an essential position in integrating security into Brazil's economy, society, and defense.

However, despite the interdependence of cybersecurity and the shared responsibility of various sectors in strengthening the digital ecosystem, the country's cybersecurity agenda remains profoundly fragmented, and sectors often find themselves isolated in their efforts due to various motives[12]— something we will explore later in this document. This fragmentation has severe consequences for Brazil's capacity to respond quickly and effectively to attacks, as well as its ability to project a sustainable, long-term vision for cybersecurity.

With this in mind, an important question remains:

---

8 MARIN, J. "Ataque hacker ao STJ é o pior da história do Brasil". **TecMundo.** 2020. Available at: https://www.tecmundo.com.br/seguranca/206233-ataque-hacker-ter-atingido-stj-pf-investiga.htm

9 BRASIL. Estratégia Brasileira para a Transformação Digital (E-Digital). 2018.

10 SHEARS, M.; SCHNIDRIG, D. & KASPAR, L. Multistakeholder Approaches to National Cybersecurity Strategy Development. **Global Partners Digital.** 2018. Available at: https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-develo-pment/

11 EGLOFF, F.J. Contested public attributions of cyber incidents and the role of the academic community. **Contemporary Security Policy**, v. 41, n.1, p. 55- 81. 2019. DOI: 10.1080/13523260.2019.1677324.

12 Public recognition of the fragmentation of the cybersecurity debate does not exclude already existing mechanisms and policies within each sector - and its importance for cybersecurity governance in the country. One example is the establishment of information security teams and plans in different Ministries with the objective of developing good practices for guaranteeing confidentiality, integrity, and information accessibility.

how can we better integrate cybersecurity agendas in Brazil? In our paper, "A Strategy for Cybersecurity Governance in Brazil",[13] we sought to map out efforts from different sectors and initiatives that sought to create intersectoral links. We identified that a large proportion of these efforts – especially those focusing on incident response and information sharing in critical moments – such as the megaevents (Rio+20, Confederations Cup, World Cup and others), were successful in consolidating good practices and institutions for initiating this intersectorial information exchange. However, when we look at the policy development processes, cybersecurity continued to be a challenging topic marking the relationship between the public sector and civil society groups.

"Cybersecurity continues to be a challenging topic marking the relationship between the public sector and civil society groups"

In this article, we focus on the E-Ciber. More specifically, we unpack the relationship between the proposals outlined in the Strategy vis à vis the emerging and existing challenges for the integration of national cybersecurity knowledge and practices. This work is the result of semi-structured and unstructured interviews with specialists from different sectors, extensive research with primary sources, as well as ethnographic work in national and international cybersecurity forums and discussions in Brazil. The next sections present the main concepts and policies, as well as identify the main gaps for building a more integrated cybersecurity governance.

13 HUREL, L.M. & LOBATO, L.C. A Strategy for Cybersecurity in Brazil. **Instituto Igarapé**. 2018. Available at: https://igarape.org.br/en/a-strategy-for-cybersecurity-governance-in-brazil/.

What is Cybersecurity?[14]

There is no consensus over the definition of cybersecurity. According to standards such as **ISO/IEC 27032:2012**, the term refers to the preservation of the confidentiality, integrity, and availability of information in cyberspace, or rather, it refers to the principles which guide cybersecurity practices and activities. The European Union, on the other hand, adopts a broader definition whereby cybersecurity is defined as those activities that are necessary for the protection of networks and information systems, the users of these systems, and other people affected by cyber threats. In this case, the ultimate objective is not the security of cyberspace in its broadest sense, but rather that of the systems, users, and information that make up, act within, and are affected by threats and cyber attacks. The United Kingdom defines the term as the protection against unauthorized access, harm, or undue use of the interconnected systems (hardware, software and associated infrastructure), of the data contained within, and of the services which make them available. This definition includes harm caused by the system operator, whether intentional or accidental, in not following security procedures or in being manipulated into provoking such harm. This definition introduces specific risk elements, damages, and impacts associated with malicious activities, including data and systems. Lastly, **Colombia** specifically states that cybersecurity should be understood as the State's capacity to minimize the level of risk to which its citizens are exposed. Its objective is to protect its citizens and "State assets", and includes a set of resources, policies, security concepts, safeguards, directives, and investigation and risk management methods to do so. At the same time this definition positions the protection of citizens as a central element to ensuring national cybersecuirty, it also restates the role of the State as the main actor in facilitating and providing this security.

In Brazil, cybersecurity refers to:

"Actions geared toward the security of operations, in order to guarantee that information systems are capable of resisting events in cyber space which are capable of compromising the availability, integrity, confidentiality, and authenticity of stored, processed, or transmitted data, and of the services which these systems offer or make accessible."

— Glossary of Security Information.

This definition repeats what has been commonly refered to as the "CIA principles" (Confidentiality, Integrity and Availability) by the information security community. However, the definition emphasizes the role of system resilience, as well as introduces, in its second part, a concern with "stored, processed, or transmitted data," a phrase incorporated directly from the Brazilian General Data Protection Law approved in 2018. Unlike Colombia or the European Union, Brazil does not refer to the role of the individual in its definition of cybersecurity.

14 ISO/IEC 27032:2012; EU (2019) Regulation (EU) 2019/881. European Parliament; Colombia (2020); Conpes 3995: Política Nacional de Confianza y Seguridad Digital. Consejo Nacional de Política Económica y Social República de Colombia; Brasil (2020). Glossário de Segurança da Informação. GSI/PR.

What is cybersecurity governance?

Cybersecurity governance[15,16] refers to a holistic and integrated vision of the security of networks, systems, and services and infrastructures in a society.

As such, **it includes the institutions, initiatives, policies, programs and other mechanisms (formal and informal) that are part of an ecosystem of distributed capacities and responsibilities regarding cybersecurity.** The National Cybersecurity Strategy, for example, is an essential component for the establishment of a vision and structure for national governance, as well as for the expansion of new horizons in capacity development. Despite being a recent term, cybersecurity governance was included, for the first time, in E-Ciber:

> Governance of the cybernetic area is related to the actions, mechanisms, and measures that should be adopted in order to simplify and modernize the management of human, financial, and material resources, and to track the performance and assess the results of efforts carried out in this field.
>
> This governance seeks to incorporate high standards of conduct in cybersecurity, and to guide the actions of public and private agents in considering the role they exercise in their organizations in accordance with the goal and nature of their business.
>
> It also includes planning geared toward the execution of programs, projects, and processes, and the establishment of directives that will guide risk management. In this context, it guides people and organizations in terms of the observance of norms, requirements, and procedures related to cybersecurity.[17]

The Green Book on Cybersecurity,[18] published in 2010, already mentioned the necessity of establishing "macro coordination and governance" that could support the development of "a series of collaborative actions between the government, the private sector, the academic community, the third sector, and society".[19] Ten years later, this took form as the first National Cybersecurity Strategy.

Over the past years, various institutions and specialists have sought to develop and articulate different concepts related to cybersecurity governance. The Global Cyber Security Capacity Centre (GCSCC) of Oxford University, for example, developed an analytical model for assessing the maturity of countries in cybersecurity (CMM). The model divides maturity into five dimensions: (i) policies and strategies, (ii) culture and society,

---

15 15 Governance is a quite controversial and highly debated concept in various disciplines. According to Rosenau and Czempiel (1992), governance is a concept which transcends the scope of the government, embracing informal, nongovernmental mechanismos within a system (whether national or international). Gbikpi e Grote (2002), on the other hand, work with the concept of participative governance, or rather, the understanding that the development of policies, in the sense of encouraging actors to articulate their interests and deliberate on common proposals, is part of the solutions for achieving sustainable public policies.

16 ROSANAU, J. N.; CZEMPIEL, E.-O. **Governance without Government: Order and Change in World Politics**. Cambridge: Cambridge University Press. 1992.
GBIKPI, B.; GROTE, J.R. From Democratic Government to Participatory Governance. Em: GBIKPI, B.; GROTE, J.R. (org.). **Participatory Governance: Political and Societal Implications**. Springer Nature. 2002.

17 Definition taken from E-Ciber.

18 Document developed and published by the Institutional Security Cabinet in 2010 which presented potential strategic directives for the establishment of the National Cybersecurity Policy over the short-, medium-, and long-term.

19 MANDARINO, R. & CANONGIA, C. **Livro Verde de Segurança Cibernética.** GSI/DSI. 2010. (Page 14)

(iii) education, (iv) legislation e (v) standards and technologies. Other organizations, such as the Potomac Institute, have developed a Cyber Readiness Index[20] to assist leaders from different countries in identifying gaps between a country's current position and the capacities required for achieving its vision of economic development.[21] These and other models have taken on an important role in consolidating the minimum parameters for cybersecurity at the national level. However, despite the diagnoses provided by them, the question remains as to how we can achieve greater integration and intersectorial exchange between different components of this cybersecurity governance.

It is important to note that governance is not restricted to the establishment of a "cybersecurity culture"[22,23] nor to raising awareness about the risks associated with the digital environment. Despite being intimately connected, governance refers to a constellation of arrangements of norms, policies, standards, and practices which coordinate and make up cybersecurity development; whereas culture refers to concepts, paradigms, ideas, narratives, and practices which are continuously, and sometimes unconsciously, molding multiple perceptions and security practices.

Governance allows us to understand culture as a component which permeates and informs the arrangements and mechanisms that can be adopted to respond to, identify, and preserve systems, networks, data, and infrastructure, as well as strengthen fundamental rights.

As the next sections show, government agencies as well as the private sector have advanced in the development of specific cybersecurity and information security policies, but this has raised new issues for the alignment of visions and for cooperation in at least three ways:

- First, a lack of alignment between public policy formulators and technical specialists working in their respective information security departments.
- Second, a lack of alignment between different agencies, associations, and sectors regarding cooperation in this area.
- Third, a lack of alignment regarding concepts and vocabulary for identifying threats and risks, as well as in designing strategies for a more encompassing cybersecurity governance in Brazil.

---

20 Cyber Readiness Index (CRI).

21 In contrast with Oxford's CMM, the Cyber Readiness Index highlights seven elements for measuring and analyzing readiness; (i) national strategy; (ii) incident response (iii) digital crime and investigations; (iv) information sharing; (v) investment in research and development; (vi) diplomacy and commerce; (vii) defense and crisis response.

22 There is no one definition of "cybersecurity culture", although two dimensions of the debate deserve mention. First, culture is associated with the intraorganizational environment. Literature on organizational studies and reports from the private sector understand culture as something centered on the "human factor" involved in cybersecurity. In establishing an organizational culture, the organization ought to consider the tacitly shared artifacts, values, and premises, as well as levels of knowledge regarding cybersecurity and information security (Van Niekerk & Von Solms, 2009). Awareness campaigns are one way of creating this culture, making information security and cybersecurity part of everyday routine (Von Solms, 2000). Second, the notion of "cybersecurity culture" arose as an international theme in 2003, with the approval of the UN General Assembly Resolution on the establishment of a global culture of cybersecurity. Since then, the document has served as a central reference in international and regional debates on the construction of cybersecurity capacities (A/RES/57/239).

23 VON SOLMS, B. Information security – the third wave? **Computers & Security.** v. 19, n. 7, p.615–20. 2000. DOI: https://doi.org/10.1016/S0167-4048(00)07021-8

Based on the already developed cyber capacities models,[24,25] studies on governance, along with semi-structured and unstructured interviews, this paper analyzes the different components of governance within the context of E-Ciber, and looks to understand how the Strategy shapes integration[26] and cooperation.

The dimensions[27] for analysing cybersecurity governance are: national and international cooperation, coordination, knowledge integration, the sustainability of efforts, and cybersecurity-related training.

All of these dimensions are intimately connected. In separating them, however, we can identify specific challenges and best practices for developing each pillar.

Cooperation (national and international) – Initiatives between different actors towards a common objective. These include not only agreements, plans, projects and operational cooperation but also the development of mechanisms to improve work across sectors, ministries, and agencies within and outside of the Federal Public Administration (FPA), as well as (formal and informal) collaborative practices among public and private actors.

Coordination – The establishment of channels, points of contact, best practices, protocols, and/or other mechanisms for coordinating activities related to cybersecurity. This coordination is further potentialized in institutional contexts with clear roles and responsibilities as well as specific intra- and interagency as well as multistakeholder mechanisms.

Capacity Building – This includes elements such as cybersecurity education and training, and activities focused on improving capacities for responding to cyber threats – such as establishing information sharing protocols across government agencies and other sectors. These are some examples of good practices adopted by different countries that enable effective circulation and communication of knowledge to support the development of well-informed threat responses.

Knowledge Integration – From response activities and incident processing to data protection and the preservation of human rights, security depends not only on articulation between different groups, but also between different forms of knowledge and expertise. This dimension includes activities that range from incident response to data protection and the preservation of human rights. Understanding how other sectors have approached cybersecurity and mapping the initiatives they have developed can help foster new avenues for trust and coordination.

Sustainability of Efforts – The development of mechanisms, partnerships, and activities that can have a long-lasting impact and/or can endure and adapt to changes in the threat and risk landscapes. Sustainability is thus understood in the broad sense, referring to financial sustainability, governance mechanisms, strategies, cooperation mechanisms, transparency and accountability measures, as well as frameworks for monitoring the implementation of activities/objectives.

---

24 "Cyber capacities" refers to the series of initiatives which seek to empower individuals, societies, and governments in enjoying the benefits of digitalization. There is no one definition of capacities. Given their subjectivity and the multiple social, economic, and political contexts and realities in which these capacities are identified, they can vary greatly depending on the country. Pawlak e Barmpaliou (2017), however, present at least five perspectives which contribute to the debate on cyber capacity building (CCB). The development definition, in line with the definition above, emphasizes how these capacities are fundamental for the sustainable development of a cybersecurity in which benefits are distributed throughout the most diverse spheres of society.

25 PAWLAK, P.; BARMPALIOU, P-N. Politics of cybersecurity capacity building: conundrum and opportunity. **Journal of Cyber Policy**. v. 2, n.1, p. 123-144. 2017. DOI: 10.1080/23738871.2017.1294610

26 In this sense, integration refers to specific indicators for the development of a more inclusive governance in cybersecurity-related themes in Brazil.

27 These dimensions were reached through the analysis of documents and interviews, as well as inspired by the following work: HOHMANN, M; PIRANG, A; BENNER, T. Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach. **GPPi.** 2017. Available at: https://www.gppi.net/2017/03/06/advancing-cybersecurity-capacity-building-implementing-a-principle-based-approach

Multistakeholder Landscape of Cybersecurity Governance[28]

Over recent years, cybersecurity has been continuously associated with a specific group of institutions: the Institutional Security Cabinet, the Armed Forces, the intelligence agencies, the Federal Police, and the computer incident response teams.[29] The Department of Information Security of the Institutional Security Cabinet (DSI) and the Armed Forces (Cyber Defense Command and the Cyber Defense Center) have been placed at the center of cybersecurity and cyber defense responsibilities and capacities. This is largely due to the rapid institutionalization of cybersecurity within these two agencies during the megaevents period (2012-2016).

The image below shows that despite the concentration of capacities in these two agencies, the responsibility, practice, and performance in cybersecurity issues depend on a larger group of actors that, over the past few years, have shaped different dimensions of this debate.[30]

Adopting a cybersecurity governance approach to the Brazilian landscape allows us to visualize security as a responsibility that goes beyond this centrality of government agencies – composed by a broader landscape of stakeholders that includes organizations from civil society, the financial sector, and other areas.[31]The figure below shows the plurality of current institutions, providing a vision of a complex field in which all of these actors (and their respective sectoral policies and norms) are positioned. The recognition of cybersecurity as a shared responsibility is the first step towards mapping gaps and identifying opportunities for strengthening the country's cybersecurity resilience.

"A governance approach allows us to visualize cybersecurity as a responsibility that goes beyond the government agencies, including organizations from civil society, the financial sector, and other áreas"

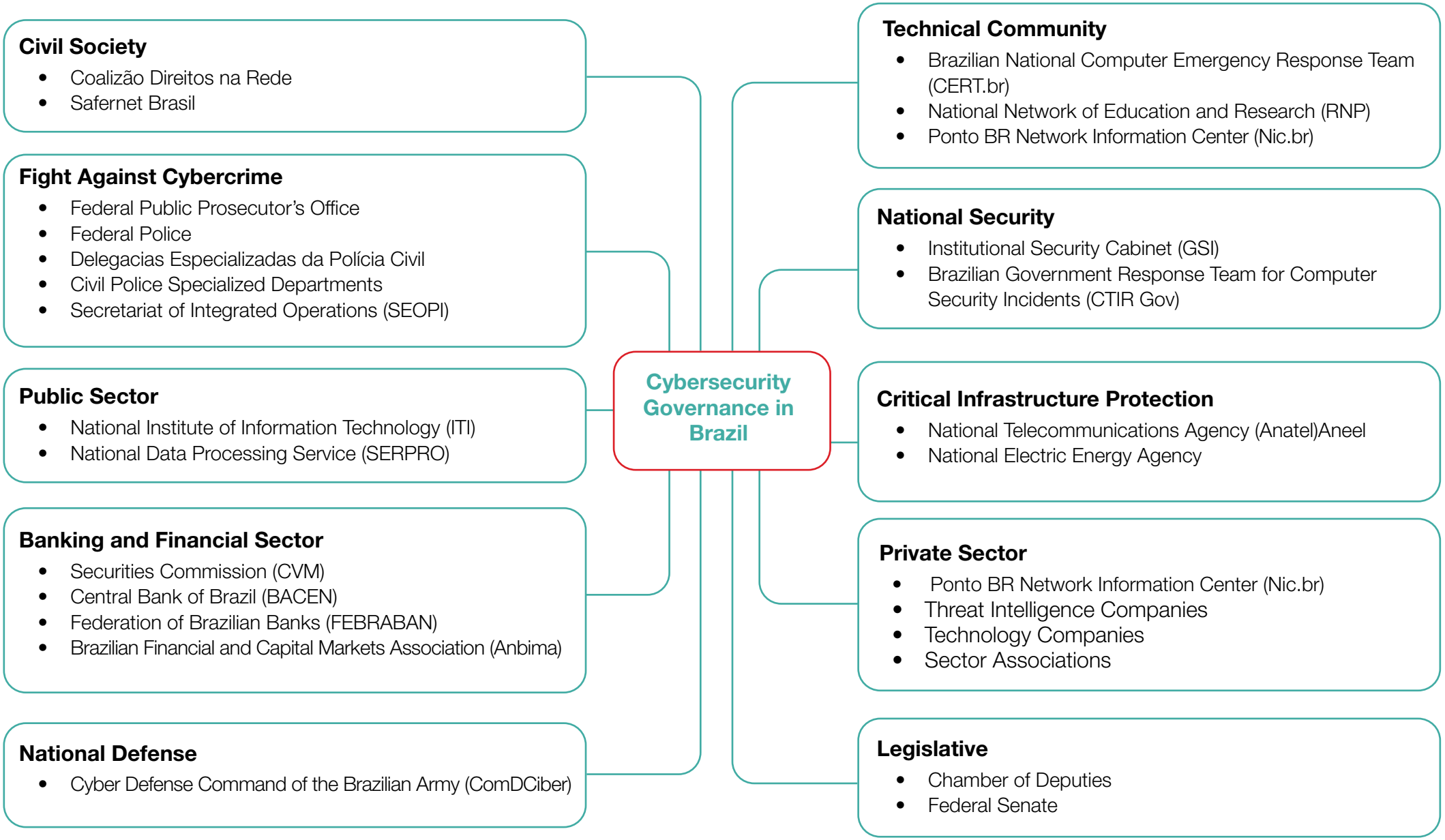
28 The image of cybersecurity governance in Brazil is not exhaustive. The selections of sectors and actors arose through the interviews, document analysis, and the mapping of initiatives in different sectors.

29 DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cyber security in Brazil: Threats and responses. Rio de Janeiro: **Instituto Igarapé,** p. 3-32. (Strategic Paper 11). 2014.

30 HUREL, L. M. "Securitização e governança da Segurança Cibernética no Brasil". In REIA, J.; FRANCISCO, P.A.P.; BARROS, M.; MAGRANI, E. (org.). **Horizonte presente: tecnologia e sociedade em Debate.** Belo Horizonte: Letramento. 2018.

31 HUREL, L.M. & LOBATO, L.C. A Strategy for Cybersecurity in Brazil. **Instituto Igarapé**. 2018. Available at: https://igarape.org.br/en/a-strategy-for-cybersecurity-governance-in-brazil/.

Cybersecurity governance in Brazil



Challenges for Cybersecurity Governance in Brazil

After three months of interviews with specialists from different sectors, along with document analysis and ethnographic work in different spaces, forums, and debates, we identified six main challenges to cybersecurity governance in Brazil that will be further unpacked in this paper, and in relation to the E-Ciber:

- The absence of a shared vocabulary when referring to cybersecurity/digital security issues in society;
- The association of cybersecurity with the subjects, responsibilities, and capacities of military institutions;
- Lack of awareness regarding specific and shared risks;
- The lack of mechanisms for sharing information regarding risks/threats as well as sharing knowledge across sectors;
- Lack of normative, strategic, and operational alignment; and
- The existence of different cybersecurity maturity levels in society.

Building a vision for cybersecurity in Brazil: E-Ciber

National cybersecurity strategies are action plans designed to improve the resilience and security of infrastructure, services, and citizens. They present the main objectives, priorities, and principles the country should achieve over the next few years.[32] Over 100 countries have already published their national strategies.[33] In Latin America and the Caribbean, 12 countries already have national cybersecurity plans and six are currently elaborating one. Brazil was the 12th country to publish its strategy.[34] Other countries, such as Colombia, have published the third edition of their strategy. Uruguay – which has one of the highest rates of internet access in the region – does not have a specific strategy, rather they encompass cybersecuirty within their Digital Agenda, which was defined by the Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC) – thus leaving cyber defense to be included in documents that are narrower in scope such as national defense policies and strategies.

These differences emphasize the fact that cybersecurity strategies ought to be understood in their respective contexts and that, despite being important indicators of a country's maturity and capacities, they cannot be reduced to a mere checklist. It therefore becomes necessary to understand how cooperation, coordination, communication, and the strengthening of relevant knowledge are operationalized within the strategies.

32 ENISA. National Cybersecurity Strategies. **ENISA**. s.d. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies.

33 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

34 OAS. Cybersecurity: Risks, Progress, and the way forward in Latin America and the Caribbean. **OAS**. 2020.

The Context

On 5 February 2020, Brazil approved its first Cybersecurity Strategy (E-Ciber). The document established the main cybersecurity actions to be carried out by the government (nationally and internationally) between 2020-2023.

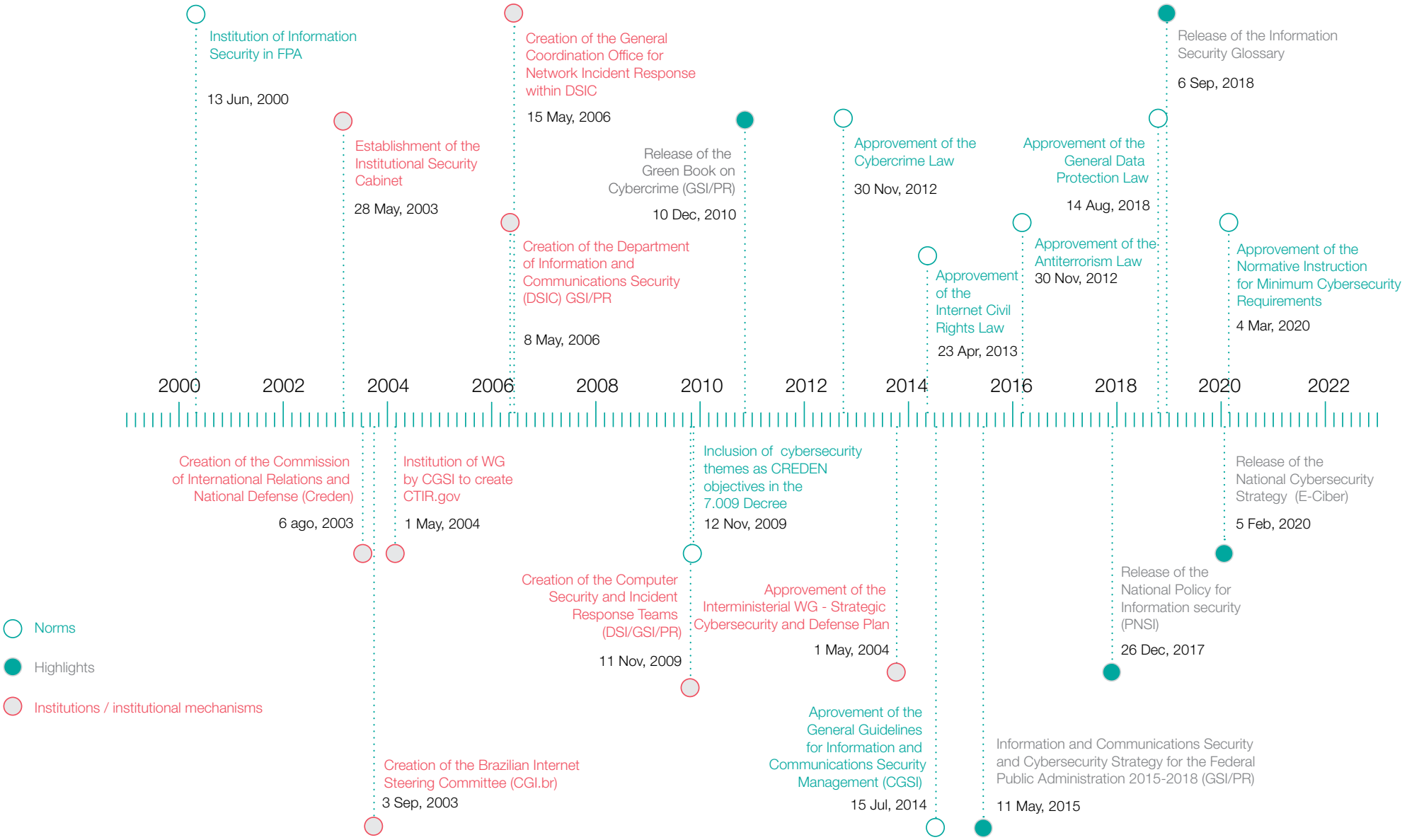
However, this is not the governments' first effort towards establishing guiding principles, competencies and objectives for national cybersecurity. Since the mid-2000s, Brazil has gradually introduced the term into its political-strategic vocabulary through the publication of various documents (White Papers) such as the Green Book on Cybersecurity (2010) and the Information and Communications Security and Cybersecurity Strategy for the Federal Public Administration 2015-2018. Different agencies within the Federal Public Administration have also sought to insert security concerns into their respective planning. Such is the case of the Digital Transformation Strategy (E-Digital), developed by the Ministry of Science and Technology and the Ministry of Communication, which included cybersecurity and cyber defense, as well as cybercrimes within its central themes regarding trust in the digital environment. Activities related to cybersecurity, however, although increasingly part of national documents and strategies, are not widely visible across different sectors of society. With this in mind, we present below two timelines with the key institutional and political developments in cybersecurity and cyber defense.

"despite being important indicators of a country's maturity and capacities, the strategies cannot be reduced to a mere checklist"

Since 2000, the government has developed institutions, policies, and directives on cybersecurity.[35] Beginning with the concept of information and communications security, it is gradually included cybersecurity in its national agenda.

35 See also: BRASIL. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018. **Gabinete de Segurança Institucional da Presidência de República.** 2015.

Timeline: Cybersecurity in Brazil (FPA)



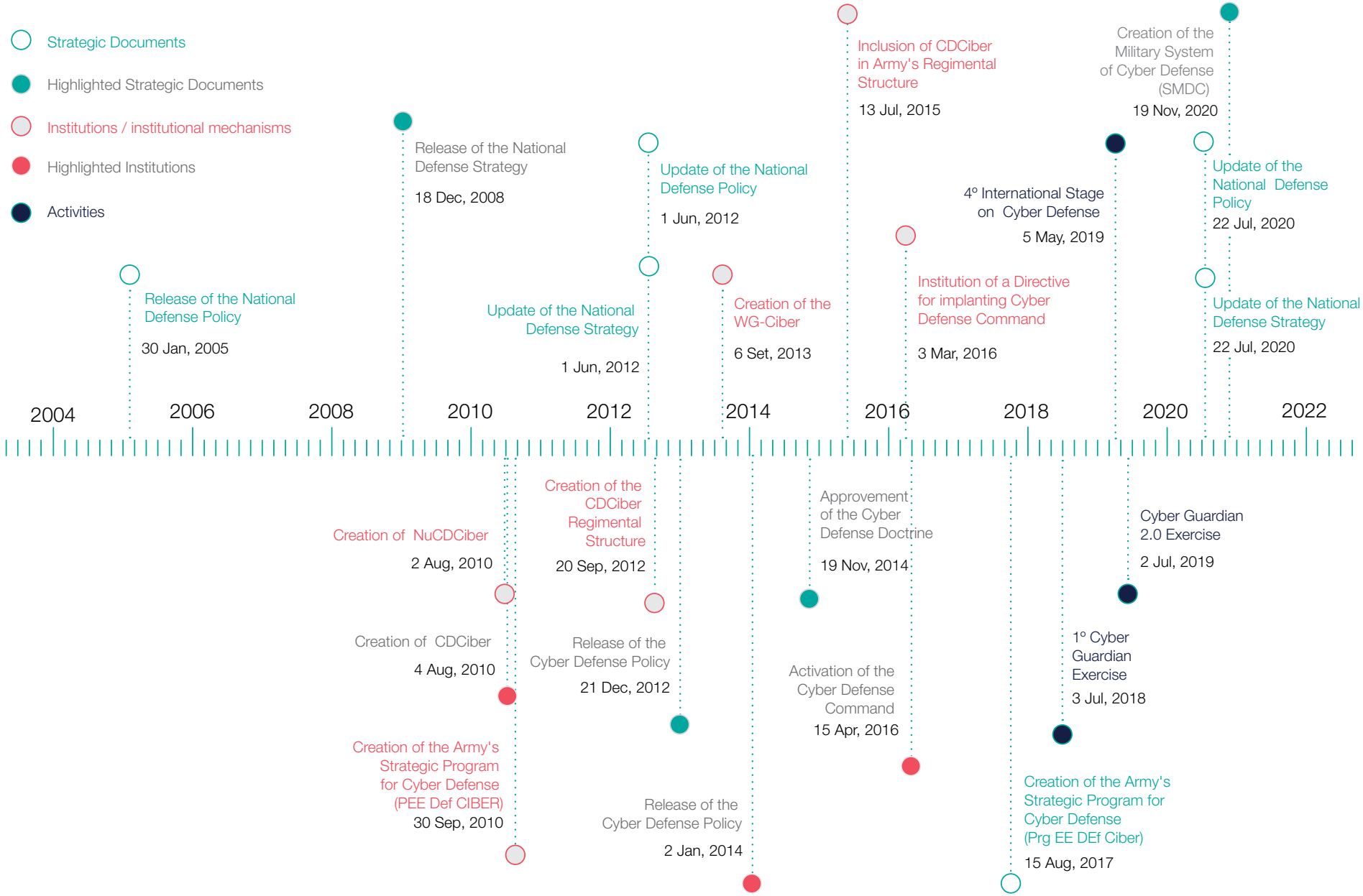
Whereas the timeline portrays more than two decades of work, in practice, the development of a legislative and normative security framework only gained greater visibility in society and legislative traction in 2012-2013 with the Cybercrime Law and the Edward Snowden revelations — both of which impacted the process of the development of the Brazilian Internet Bill of Rights. Since then, there has been a transition within the normative/regulatory environment: (i) greater specification of the normative vocabulary used to address digital and cybersecurity issues. The Brazilian Data Protection Law, for example, brings a more fine grained perspective on data protection and security; there has also been a gradual advancement in consolidating sectoral policies, such as the Central Bank resolution on cybersecurity for the financial market.[36]

Between 2010 and 2020, GSI presented a series of documents which gradually inserted cybersecurity into its range and scope of activities. This includes: the proposal for the development of a strategic vision for cybersecurity(Green Book on Cybersecurity), a document dedicated to exploring the relationship between information security and cybersecurity in the Federal Public Administration, a glossary of terms, and, more recently, the National Information Security Policy (PNSI) and E-Ciber.

For more than 10 years, Brazil has invested in developing its cyber defense capacities, starting with the recognition of the cybersecurity sector as one of the strategic pillars for of national defense in the 2008 National Defense Strategy. According to the Cyber Defense Doctrine, the term refers to a "set of offensive, defensive, and exploratory actions carried out in cyber space and in the context of national strategic planning, coordinated and integrated by the Ministry of Defense with the objective of protecting information systems of interest to National Defense, obtaining data for the production of intelligence, and compromising the information systems of the opponent."

36 DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cyber security in Brazil: Threats and responses. Rio de Janeiro: **Instituto Igarapé**, p. 3-32. (Strategic Paper 11). 2014;.
HUREL, L. M. "Securitização e governança da Segurança Cibernética no Brasil". In REIA, J.; FRANCISCO, P.A.P.; BARROS, M.; MAGRANI, E. (org.). **Horizonte presente: tecnologia e sociedade em Debate.** Belo Horizonte: Letramento. 2018.

Timeline: Cyber Defense in Brazil



As shown by the timeline above, there was a greater concentration of efforts in the period between 2010 and 2016 — while the country was preparing for the cycle of megaevents to be held in the country (Rio+20 being the first and the 2016 Olympics the last). This period also saw the development of fundamental documents for helping and guiding strategic cyber operations in Brazil (such as the Cyber Defense Policy and the Cyber Defense Doctrine) as well as institutions dedicated to the operationalization and implementation of cyber defense activities (the Cyber Defense Center and Cyber Defense Command).[37]

On the one hand, the megaevents were an important contextual trigger for investments in cybersecurity and cyber defense – which resulted in greater capacities development of strategic actors. To respond and prepare for these events, the Armed Forces (especially the Army) had to establish joint coordination structures in order to protect systems and networks during the events. This resulted in the consolidation of communication channels with agencies such as the Federal Police, CERT.br, CTIR.gov and others.

After the megaevents, two dynamics began to take shape: (i) the consolidation of cyber defense programs and budgets (ii) a focus on coordination within the Ministry of Defense - one example being the approval of the Military Cyber Defense System in November 2020 — and between agencies, through activities such as the "Guardião Cibernético" exercise.[38]

However, despite this period having resulted in greater operational coordination and cooperation, it has also left a legacy of a militarized version of cybersecurity that has received critiques from civil society groups as well as from the academic community.[39]

Next Steps

With E-Ciber published in the beginning of 2020 and a National Cyber Security Law or Policy (to be defined),[40] Brazil has the opportunity to integrate the experience of these agencies and their best practices within other sectors' experiences and coordination mechanisms.

While these different initiatives have created an ecosystem of approaches for strengthening resilience and cybersecurity in the country, little has been said about the synergies and gaps that exist between these efforts. As demonstrated by the attack on the STJ in November 2020, the lack of basic preparation and care in updating systems can generate an unprecedented impact for the functioning of agencies which are critical to Brazilian democracy. It is therefore paramount that the attention stemming from these attacks serve as an important sign, not only of the necessity of improving the incident response channels, but also that of coordinating and aligning different sectors.

The General Data Protection Law (LGPD) was an important step toward the consolidation of specific security provisions regarding data security for businesses and State entities. **LGPD, in its Art. 6, highlights security as one of the essential principles for treating personal data. It also defines it as the** "use of technical and administrative measures apt for protecting personal data from unauthorized access and from accidental or illicit destruction, loss,

37 https://www.eb.mil.br/web/imprensa/aviso-de-pauta/-/asset publisher/0004ie79MBVM/content/exercicio-guardiao-cibernetico-2-0.

38 Nota técnica da Sociedade Civil para a CPI de Crimes Cibernéticos. **Coding Rights e Instituto Beta para Internet e Democracia.** 2016. Available at: https://cpiciber.codingrights.org/crimes-ciberneticos/; ARTIGO 19. "Da Cibersegurança à Ciberguerra - do desenvolvimento de políticas de vigilância no Brasil." **Artigo 19.**

39 DE LUCA, C. "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". **Tilt UOL.** 2020. Available at: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

40 Currently, Art.48 §1 states that "communication [of the incident] will be made within a reasonable timeline, as defined by the national authority".

alteration, communication, or diffusion." **It also requires that businesses adopt technical and administrative security measures to protect against incidents (Art. 46) and determines that incidents must be reported to the National Data Protection Authority** and to the data subject (Art. 48). Despite attempts to delay the applicability of LGPD during the pandemic, its coming into effect in August 2020 contributes to the consolidation of good security practices regarding the processing, storage, and transmission of personal data.

However, new challenges have arisen for data security. These challenges are directly linked to the maturity of cybersecurity in the country, which includes, for example, the development of a policy for sharing vulnerabilities and incidents within the public sector with deadlines for communicating them. [41] The United Kingdom, for example, published a public note explaining how it handles vulnerabilities. Mechanisms like this provide greater transparency and predictability for cybersecurity governance in the country.[42]

The E-Ciber is the first document dedicated to developing objectives and actions for consolidating cybersecurity in the country. It also opens up a path ahead for a reflection on how to integrate sectors, as well as harmonize different, existing legislation through the consolidation of a macropolitical vision for the country.

The strategy

Six days prior to the end of Michel Temer's administration, **in December 2018,** a decree approving the **National Information Security Policy (PNSI) was published.**[43] After a decade of ad hoc development and proposals for the consolidation of a national policy dedicated to the theme, the PNSI introduced a proposal for developing strategies for addressing specific Information Security issues. Developed by the Institutional Security Cabinet of the President Presidency of the Republic (GSI/PR) — the main agency in charge of developing related policies and directives — PNSI anticipates the establishment of five strategies: (i) cybersecurity; (ii) cyber defense; (iii) critical infrastructure security; (iv) confidential information security; and (v) protection against data leaks.

PNSI establishes a strategic horizon for cybersecurity, guaranteeing some degree of predictability in the actions of agencies such as GSI in a moment of political instability and economic uncertainty. Beyond this, PNSI not only foresees the **elaboration of strategies, but also national plans to guide the implementation of actions for cybersecurity in the country.**

However, this was not a novel development. The PNSI builds on previous recommendations from other documents, in particular, from the Green Book on Cybersecurity of 2010. The aim of the Book was to provide support for the government in the elaboration of a National Cybersecurity Policy. At the time, the document already stated that the National Policy should be "as far as possible, preceded by analysis and consensus constructed with stakeholder participation for the viability and optimization of the full process, thus creating a

41 LEVY, I. Equities Process: Publication of the UK's process for how we handle vulnerabilities. **NCSC.** 2018. Available at: https://www.ncsc. gov.uk/blog-post/equities-process

42 Decree n.9.637 of 26 Decembro 2018.

43 Decree n.9.637 of 26 December 2018.

political-strategic and technical State Agenda."[44] Despite the ten-year gap between the Green Book and the E-Ciber, shortly after the launch of the Strategy, GSI representatives had already mentioned that a policy was being developed.[45]

In line with the PNSI, the E-Ciber was the first (out of five) module to be developed and approved. It is considered the prime example for the country's approach to information security. The Strategy is the result of seven months of work, 30 days of closed meetings, and 20 days of public consultations (166 contributions). E-Ciber adopts a similar methodology to that of the Brazilian Strategy of Digital Transformation (E-Digital), released in 2018 by establishing different axes. It defines central themes and transformations for diagnosing the national landscape. The document establishes three strategic objectives and ten strategic actions (Figure 1).

It is worth noting that the public consultation process is an important step for an agency like the GSI. It signals a willingness to incorporate society's recommendations through transparent and accessible means of participation. However, this is only one measure: the consultation began 10 September 2019 and continued through 1 October 2019, providing less than 30 days for society to contribute. As in other cases of public consultations, another issue that arose was the lack of transparency regarding how these comments were incorporated into the final text. Public consultations are one among many mechanisms available for elaborating policies and directives, and Brazil must guarantee that the operationalization and revision of the Strategy's provisions also lead to the effective integration of different sectors.

"Brazil must guarantee that the operationalization and revision of the Strategy's provisions also lead to the effective integration of different sectors"

44 MANDARINO, R. & CANONGIA, C. **Livro Verde de Segurança Cibernética.** GSI/DSI. 2010. (Page 25).

45 DE LUCA, C. "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". **Tilt UOL.** 2020. Available at: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

Figure 1: E-Ciber Objectives and Actions

Strategic Objectives	Central Themes	Strategic Actions[46]
1. Make Brazil's digital environment more prosperous and more credible 2. Increase Brazil's resilience to cyber threats 3. Strengthen Brazil's engagement in cybersecurity at the international level	**Protection and Security** • National Cybersecurity Governance (1.1)[47] • Protection from and mitigation of cyber threats (1.2) • Strategic protection (1.3) **Transformations** • Normative Dimension (2.1) • Research, Development, and Innovation (2.2) • International (2.3) • Education (2.4)	1. Strengthen cyber governance activities 2. Establish a centralized governance model at the national level 3. Promote a participatory, collaborative, credible, and secure environment between public sector, private sector, and society 4. Increase government's level of protection 5. Increase level Critical National Infrastructure protection 6. Improve legal cybersecurity frameworks 7. Incentivize innovative cybersecurity solutions 8. Increase Brazil's international cooperation in cybersecurity 9. Increase cybersecurity partnerships between public sector, private sector, academia, and society 10. Increase society's cybersecurity maturity level

46 Numbering included in Strategic Actions for the sake of analysis and reference. In the original text, the strategic actions were numbered differently. Here we have adopted a simplified numbering for ease of access. For a more detailed vision of the strategic actions and their respective recommendations, see Annex 1.

47 Numbering matches the text of E-Ciber.

The Institutional Security Cabinet, responsible for developing E-Ciber and the future national cybersecurity policy. It will also facilitate coordination among different sectors. There are still considerable challenges regarding GSI's role and the implementation of E-Ciber. As much as GSI already carries out the role of coordinating and facilitating actions within the FPA, its relationship with civil society remains fragile, with groups frequently pointing out the lack of transparency and the militarization of the GSI's Information Security Department's agenda.[48] New formal and informal channels could help to build trust between the different actors, but the implementation of key actions and the achievement of objectives, such as the establishment of a National Council with different sectors (as laid out in E-Ciber), is largely viewed with skepticism. The carrying out of E-Ciber will require a continuous effort from all sides.

The Strategy has also received criticism for being more of a diagnosis of the country's cybersecurity situation, or even "a letter of good intentions" — something already accomplished by the Green Book of Cybersecurity of 2010

— than an operational document with clear goals and guidelines for implementation.

Despite E-Ciber seeking "to represent the federal government's perspective on" the subject,[49] the horizon for its implementation Strategy remain undefined. The United Kingdom's national cybsersecurity strategy, for example, presents both a diagnosis of the state of technology and of the strategic environment and well as it includes clear indications regarding "plans of implementation," "results evaluation," and guiding "objectives and principles" which define the government's relationship with other sectors.[50]

48 Also called a "whole-of-society" or "whole of nation approach". Klimburg (2011) argues that the cyber power of a nation is composed of three dimensions: coordination of political-normative and operational aspects between governmental agencies, policy coherence through international alliances and legal frameworks, and cooperation with non-state actors. These non-state actors (private sector and civil society) possess important capacities and have a proximity to different realities and risks regarding diverse sections of society. Uniting these different sectors is not simply a measure of inclusion, but, as noted in Klimburg (2011), it is the foundation of a "whole of nation approach", which is a central element in defining the cyber power of a nation. In this way, beyond operational and normative capacities, "power" is determined by the State's capacity to interact, integrate, and learn with these sectors when forming its own position.
KLIMBURG, A. Mobilising Cyber Power. **Survival.** v.53, n.1, p.41-60. DOI: 10.1080/00396338.2011.555595.

49 Cyber Security Summit Brasil. Available at: https://www.youtube.com/watch?v=TUv4wcfb-AY

50 UK. National Cyber Security Strategy 2016-2021. P. 9. Available at: https://www.gov.uk/government/publications/ national-cyber-security-strategy-2016-to-2021

Dimensions of Cybersecurity Governance[51, 52]

In this section, we will present an analysis of E-Ciber (strategic actions and recommendations) in accordance with the five dimensions of cyber governance outlined in the beginning of this document: **cooperation, training, coordination, knowledge integration, and sustainability of efforts.** After conducting a thematic analysis of the document, it becomes clear that many of the strategic actions and recommendations interact with different dimensions of cybersecurity governance, while cooperation and **sustainability of efforts** represent the more transversal elements of the Strategy. **Coordination,** however, stands out for presenting more concrete actions, indicating possible, practical developments for E-Ciber in the legislative sphere, and emphasizing the role of GSI and other institutions in guaranteeing cybersecurity. Recommendations associated with **capacity building** and **knowledge integration** introduce more principles-based suggestions regarding the adoption of technological standards, as well as proposing the use of existing frameworks in order to facilitate the integration of other sectors in the cybersecurity debate.

Cooperation

Initiatives between different actors towards a common objective. These include not only agreements, plans, projects and operational cooperation but also the development of mechanisms to improve work across sectors, ministries, and agencies within and outside of the Federal Public Administration (FPA), as well as (formal and informal) collaborative practices among public and private actors.

National Cooperation

The Strategy presents two dimensions of cybersecurity cooperation. On the national level, the document emphasizes the necessity of establishing channels for **sharing information** about incidents, vulnerabilities, and risks both within the FPA as well as between the private and public sectors. [53] In the FPA, data sharing is regulated by the Decree 10.046, from 2019, which defines the governance of data sharing. More specifically, the Decree establishes levels of data sharing (broad, restricted, and specific) in accordance with its confidentiality. Parameters like these can and should inform the development of specific practices regarding incidents and vulnerabilities identified in different sectors within the FPA. Despite the sensitive nature of this kind of information, this cannot be an obstacle to addressing the objectives laid out in the E-Ciber.

However, there are main two challenges to meeting information-sharing objectives. The first refers to the fact that the sharing of vulnerabilities and information related to incidents is not a consolidated practice within the FPA. There are various reasons for this: the absence of networks of trust, the lack of clear information

51 The strategic actions were allocated to each dimension in accordance with two criteria: explicit mention of the elements contained within the definition of the dimension in the description of the strategic action, and/or in the initiatives which were suggested and identified in each of the strategic actions.

52 The central themes were allocated to each dimension in accordance with their relation to the definitions of the dimensions. Not all of the elements that were included among the “central themes” are explicit recommendations, but rather suggestions for developing each theme.

53 Strategic actions which include explicit recommendations on information sharing: AE3 (encourage sharing information about cyber incidents and vulnerabilities; establish mechanisms which allow for interaction and knowledge sharing on different levels) and AE9 (encourage the creating of information sharing mechanisms regarding cyber risks).

sharing mechanisms – such as a shared and widely disseminated protocols and/or policies – the inexistence of designated points of contact for receiving and communicating with different government agencies, and financial resources for establishing specific teams to work on operationalizing these initiatives. However, as the attacks on the STJ in November 2020 demonstrated, the costs and impacts of this lack of national information sharing protocols can harm the very functioning of the country's democratic institutions.

The second challenge is that there are still no specific regulations for sharing information on incidents and vulnerabilities between the public and private sectors. This is concerning in that many businesses not only possess knowledge and capacities for identifying threats, but much of the country's critical infrastructure rely on the technologies and services provided by these businesses. The exclusion of the private sector contributes to increased gaps in knowledge regarding threats in the public sector, thereby diminishing its capacity to adequately respond to incidents.

Information sharing can be strengthened through the establishment of specific policies such as sectoral protocols. In the financial sector, for example, the Central Bank's Resolution (BACEN) 4.658 published in 2018 determines that financial organizations ought to develop initiatives for incident information sharing. At the international level, the Financial Services Information Sharing and Analysis Center (FS-ISAC) is one example of an organization dedicated sectorially addressing cyber risks through the dissemination of information sharing practices across the community.

Designating levels for sharing (within and among sectors) is worth considering in order to create trust between agencies and sectors. This practice has already been established in internationally renowned organizations such as FS-ISAC and the Forum of Incident Response and Security Teams (FIRST Org). In both cases, the organization members use Traffic Light Protocol to signal the degree of sharing of a determined piece of information by using colors (red, yellow, green, and white).[54]

The establishment of specific policies for disclosing vulnerabilities[55] can also contribute to strengthening the resilience of government services and activities, as well as encourage collaboration between FPA agencies in order to monitor and consolidate information regarding the FPA's threat landscape. Best practices in information sharing when coupled with vulnerability disclosure can also become an important mechanism for ensuring greater transparency in national cybersecurity while also building trust with other sectors and as a result from establishing consistent channels of public accountability.[56]

54 In the case of FIRST, a detailed description of TLP can be found here: https://www.first.org/tlp/ ; FS-ISAC includes TLP as a fundamental element of its "trust model" and can be accessed here: https://www.fsisac.com/tlp . Organizations such as CTIR.Gov and CERT.br use TLP as a protocol for information classification.

55 Providing information on vulnerabilities to third parties who were previously unaware of the fact. The individual or organization responsible for this is called the "reporter" (https://cyber.dhs.gov/bod/20-01/. Definition from ISO/IEC 29147:2018).

56 Some examples of established government practices regarding vulnerability disclosure include the Vulnerability Disclosure Toolkit released by the United Kingdom's National Cybersecurity Centre (NCSC) and recommendations from the USA's Cybersecurity and Infrastructure Security Agency's (CISA) recommendations regarding the publication and development of a vulnerability disclosure policy.

International Cooperation

E-Ciber has moved forward in proposing a specific, strategic action for **Brazil's international cooperation and in the area of cybersecurity.** Little is written about cyber diplomacy in the country, mostly due to the fact that it is such a recent issue (both as a field and as a practice among states). [57]The E-Ciber provides for a more robust vision regarding the future of cyber diplomacy in that it recognizes international cooperation in the text and highlights specific recommendations for advancing a structured agend on the topic.

Regarding international cooperation, E-Ciber emphasizes activities such as international exercises, cybercrime collaboration, and the consolidation of a Brazil's foreign policy in this area. With regards to cybersecurity exercises, in 2019, ComDCiber participated in the 4th International Cyber Defense Competition, which included military units from ten different countries.[58]

Brazil has also been an active player in combatting cybercrime, including its participation in specialized cybercrime groups at the Organization of American States (OAS), Europol, Ameripol, and Interpol.[59] The country's accession to the Budapest Convention was an equally important step in advancing international cooperation in this area.

The process gained traction in July 2019 and, in December of that same year, the Ministry of Foreign Relations (MRE) and the Ministry of Justice and Public Security published a note announcing its inception. In July 2020, the text was finally sent to the Senate.[60] The advancement of the accession process is in line with the recommendations laid by the E-Ciber, in particular when it refers to "increasing the use of international mechanisms to combat cybercrime".

The Ministry of External Relations has also increased its involvement in international cybersecurity. In 2020, Brazil designated its first cyber diplomat, who will be responsible for accompanying national and international developments related to international peace and security agendas. Many countries have already appointed their own cyberdiplomats and assembled specific teams within their Ministry of Foreign Affairs to articulate more purposefully their countries' national interests in global cybersecurity. Other countries, such as Denmark, have even appointed their first diplomat for big technology companies, thus liaising and cooperating with the Silicon Valley. There are various international initiatives and multilateral processes in which these diplomats have been regularly involved: the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group on the Developments in the Field of ICTs in the Context of International Security.

At the multilateral level, **Brazil was the second country to serve twice** as the chair of the UNGGE. Established in 1999, UNGGE is one of the key international spaces for debates concerning peace and security in cyberspace – focusing on the responsible behavior of States.

---

57 Australia, for example, appointed its first cyber diplomat in 2017 and, in the same year, published a specific strategy for the country's international actions entitled "Australia's International Cyber Engagement Strategy." The document covers areas such as cybersecurity, cybercrimes, digital commerce, internet governance, and others. In 2019, the country published a report on the implementation of this strategy, as well as its position on the applicability of international cyber space law.

58 ASCOM. Competição virtual envolve militares de dez países durante Estágio Internacional de Defesa Cibernética. **Ministério da Defesa.** Available at: https://www.gov.br/defesa/pt-br/assuntos/noticias/ultimas-noticias/competicao-virtual-envolve-militares-de-dez-paises-durante-estagio-internacional-de-defesa-cibernetica.

59 OAS/GCSCC. **Cybersecurity Capacity Review:** Federative Republic of Brazil. Organization of the American States. 2020. Available at: http://www.oas.org/en/sms/cicte/docs/ENG-CYBERSECURITY-CAPACITY-REVIEW-BRAZIL.pdf.

60 https://www.in.gov.br/en/web/dou/-/despachos-do-presidente-da-republica-268441788.

At the regional level,[61] Brazil has also participated in the cybersecurity Confidence-Building Measures working group[62], established in 2017 within the auspices of the Organization of American State's Inter-American Committee on Terrorism. [63] In 2018 and 2019, the working group agreed that member-states would designate a Point of Contact (PoC) to discuss the impacts of hemispheric cyber threats and to facilitate regional cybersecurity cooperation.[64]

Despite Brazil's increased participation in international forums, there are other dimensions of the E-Ciber's strategic objective on international cooperation that deserve greater attention, such as **"increasing cybersecurity cooperation agreements" and "promoting international events and exercises related to cybersecurity."**[65] Since 2013, various Brazilian joint statements and actions plans have included cybersecurity and cyber defense, cybercrimes, and the preservation of human rights as important pillars of bilateral cooperation. However, little is known about the progress of these collaborations.

As the country expands its engagement in cybersecurity, other sectors can support the consolidation of the country's foreign policy. The United Kingdom, for example, established a Multistakeholder Consultative Committee to inform the country's cyber diplomacy. In Brazil, the telecommunications regulator (Anatel), has established Brazilian Communication Commissions (CBC)[66] which are thematic groups "charged with organizing work in international telecommunications forums". The Commissions are open to the participation of actors from different sectors – one of which is dedicated specifically to "International Governance and Regimes". Initiatives such as these can improve knowledge integration, connection of specialists, as well as help enhance collaboration for consolidating foreign policy and strengthening channels for international cooperation.

Capacity Building

This includes elements such as cybersecurity education and training, and activities focused on improving capacities for responding to cyber threats – such as establishing information sharing protocols across government agencies and other sectors. These are some examples of good practices adopted by different countries that enable effective circulation and communication of knowledge to support the development of well-informed threat responses.

E-Ciber's **strategic actions** [67] highlight three key priorities for enhancing cybersecurity capacities in society: (i) adherence to technological standards (AE1); (ii) developing and updating norms for facilitating responses both to incidents and cybercrimes (AE6); (iii) investing in knowledge and in preparing teams and sectors to face cyber risks (AE7).

---

61 OAS/IDB. Cybersecurity: Risks, Progress, and the way forward in Latin America and the Caribbean. Organization of the American States. 2020. Report.

62 Confidence-Building Measures.

63 http://www.oas.org/en/sms/cicte/Documents/Sessions/2018/FINAL/RES%201%20Resolución%20Medidas%20Regionales%20de%20Fomento%20CICTE01217E.doc.

64 CICTE/RES.1/18 e CICTE/RES.1/19

65 From text of E-Ciber.

66 https://antigo.anatel.gov.br/institucional/comissoes-brasileiras-de-comunicacao-cbcs

67 Especially AE1 (strengthen cyber governance actions), AE6 (improve cybersecurity legal framework) and AE7 (Incentivize innovative cybersecurity solutions).

Standards

Technological standards are fundamental for the interoperability and security of systems and networks. Moreover, standards mold not only the physical and virtual world, but also our social relations, our way of seeing the world and the security of technologies therein. [68] This equally applies to encryption. The widespread adoption of encryption standards by the public and private sectors can promote greater confidence on the part of the population and of those who manage a system's security. According to *Cybersecurity Capacity Review,* released by Oxford University, different sectors within Brazil have already adopted different information and cybersecurity standards — the financial and electronic communications sectors among the first. The Strategy highlights **three points** which ought to define the priorities for Brazil's inclusion of, investment in, and adherence to elevated cybersecurity standards.

The first refers to **the need to establish minimum cybersecurity requirements when closing new contracts.** Over recent years, Brazil has developed sectoral policies and directives which, despite becoming increasingly more common, still need to be better incorporated within a strategic vision. Such is the case of Central Bank Resolution 4.658, which establishes a cybersecurity policy and requirements for financial institutions contracting data processing and storage services in the cloud. While the resolution was an important step towards establishing a baseline for security in the financial sector, it was criticized by the challenge it presented to smaller organizations that did not possess the resources, capacities, or expertise needed to meet specific demands, such as the establishment of incident response plans (Art. 6) or practices related to the confidentiality, integrity and availibility of data and information processed or stored by service providers (Art. 12). Despite these challenges, in December 2020, the government published the "Guide to Good Practices for Specifying Information Security and Privacy Requirements in Information Technology Contracts" to help public institutions in identifying minimum security requirements for the acquisition of technological solutions.

The second, and perhaps the main achievement of E-Ciber, was the **recognition of encryption as a central element to achieving various strategic actions.** More specifically, it emphasizes the necessity of encouraging the development of encryption skills and solutions across the whole of society, and, more specifically, for the communication of sensitive information. However, there are still significant challenges for carrying this out in practice. The troubled history of the public debate on encryption is marked by the "WhatsApp Bans" of 2014[69] and a constant tension between law enforcement access to data and the strengthening of information security through widespread adoption of encryption.[70] While countries such as the United Kingdom, USA, and Australia have favored exceptional data access for criminal persecution, Brazil has not imposed normative restrictions or regulations for encryption. On the contrary, according to a report by IP.rec (Recife Institute of Research in Law and Technology), "Brazilian Key Public Infrastructure (ICP-Brasil), a public agency created by MP n. 2.200-2/2001, established minimum recommended security standards and algorithms for encryption technologies in the country. Although there is a lack of regulation,

68 BUSCH, L. **Standards**: Recipes for Reality. Cambridge: MIT Press. 2011.

69 The private messaging app, WhatsApp, was blocked nationwide by four judicial decision when the company refused to hand over private content related to penal processes and inquiries. As noted by Jacqueline Abreu (2017:27), "It was a conflict between the traditional powers of the State, which investigate and punish through the penal process, and the growing power of information technology companies, which create and facilitate spaces for communication and the exercise of liberties."; ABREU, J. **Passado, presente e futuro da criptografia forte:** desenvolvimento tecnológico e a regulação. Revista Brasileira de Políticas Públicas. v. 7, n.3. 2017.

70 ABDELSON, H; ANDERSON, R.; BELLOVIN, S.M.; BENALOH, J.; BLAZE, M.; DIFFIE, W.; GILMORE, J.; GREEN, M.; LANDAU, S.; NEU MANN, P.G.; RIVEST, R.L.; SCHILLER, J.I.; SCHNEIER, B.; SPECTER, M.; WEITZNER, D.J. (2015). **Keys Under Doormats:** Mandating insecurity by requiring government access to all data and communications. Cambridge, 2015. Available at: https://dspace.mit.edu/handle/1721.1/97690.

there is an agenda to promote the use of progressively advanced techniques." [71] Despite this, in 2020, researchers discovered that, for over 60 years, the Army, Ministry of Foreign Affairs, and Navy used equipment and services provided by Crypto AG, an agency connected to the United States Central Intelligence Agency (CIA), and which included errors in its code in order to allow for backdoor access.[72] The disparity between Brazil's commitment to high cybersecurity and information security standards vis à vis the implementation of encryption practices remains considerably unmended with no established public consensus.

Lastly, the third and final dimension of capacity building presented by the Strategy was the **importance of international interoperability.** Efforts to increase Brazil's level of maturity depend on its adherence to international standards that allow for greater interoperability not only at the technical level but also in promoting new avenues for sharing digital risk methodologies that can enhance threat awareness. As stated in E-Ciber "it was confirmed that the adoption of unique, exclusive standards of governance do not necessarily yield positive results, when considering the

transversality and capillarity of cybersecurity activities in public and private institutions, as well as in society in general." The Strategy makes important advancements in presenting a range of standards that range from technical (encryption and common vulnerabilities exposure) to principles-based (privacy by design and privacy by default), professional (training through international cybersecurity certifications) and methodological (risk assessment frameworks). However, despite highlighting examples of international standards and national experience, the Strategy does not present a roadmap or guideline for achieving these objectives. In the recommendations, the document returns to a "list of intentions" model and fails to effectively communicate how the government will support these processes. Despite the objectives being more directed toward the FPA, national and international interoperability can only be achieved through the establishment of interagency and multisectoral communication and trust.

As the landscape presents different levels of maturity and resources, it is important that the strategic vision of standard-setting be accompanied by investments in educational programs and plans with resources for the federal and state levels – such as establishing clear goals for implementing standards (minimum security criteria) over a previously-determined period of time.

To carry out this plan, **it is important to establish minimum standards, with the necessary adaptations to the realities of different agencies, to run a diagnostic which portrays the current** situation of the agencies and states, and to develop an implementation plan with defined short-, medium-, and long-term priorities.

Other immediate possibilities include, for example, defining metrics and standards for agencies and departments within the FPA. These and other measures can facilitate better tracking of the strategic objectives across the government and ultimate inform their achievement. If no progress-tracking mechanisms are put in place, by the end of the timeframe of the E-Ciber (2023), the government will not have specific metrics for evaluating the true advancement of strategic objectives and actions – further reinforcing critiques to the strategy for being a list of intentions rather than a vision that could link to concrete implementation activities.

---

71 RAMIRO, A.; CANTO, M.; LIMA, J.P. & AGUIAR, T. **O Mosaico Legislativo da Criptografia no Brasil:** uma análise de projetos de lei. Instituto de Pesquisa em Direito e Tecnologia do Recife. 2020. Available at: https://ip.rec.br/publicacao/o-mosaico-legislativo-da-criptografia-no-brasil-uma-analise-de-projetos-de-lei/.

72 BRUSTOLIN, V.; DE OLIVEIRA, D. & PERON A.E.R. Exploring the relationship between crypto AG and the CIA in the use of rigged encryption machines for espionage in Brazil, **Cambridge Review of International Affairs.** 2020. DOI: 10.1080/09557571.2020.1842328.

Norms

The Strategy specifically dedicates one strategic action to improving the current cybersecurity legal framework (AE6[73]). Of the six recommendations listed in the strategic action, three are directly related to developing capacities: **identifying gaps in the current legislation, working to include new types of cybercrimes, and elaborating norms focused on emerging technology.** While interest in and attention to themes related to cybercrime, information security, and information security have gained increasing notoriety in society, there is little discussion about training public policy makers and legislators to work with these themes.

Knowledge and preparation for teams and sectors

Beyond training policy- and decision-makers, the Strategy also presents recommendations for the private sector and society. [74] For the public and private sectors, it highlights the necessity of activities such as internal awareness campaigns and the professionalization of employees working in cybersecurity and cybercrime. In contrast, a large percentage of the recommendations directed towards the 'society' focus on strengthening cybersecurity education, from early childhood through graduate-level programs.

Two points merit attention as potential gaps in the E-Ciber's approach to capacity building: First, the lack of inclusion of an interdisciplinary cybersecurity vision that recognizes the role the social sciences, in educational and professional programs. . Integration of different types of expertise in capacity building processes is key element for adequately preparing public, private and civil society actors to understand the geopolitical, social, economic, and legislative dynamics in which security technologies and practices develop (whether national, individual, or social). Second, the often-overlooked role of civil society in cyber capacity building processes.

This gap also draws from a deeper absence of civil society from the Strategy. The E-Ciber does not refer to " civil society", only "society" or "society in general". **It is important to note that** civil society groups have played an key role in organizing digital security programs, courses, and awareness campaigns for risk groups, vulnerable communities, investigative journalists, and other segments of the population.[75] Recognition of this role can be an important step in strengthen training capacities.

Coordination

The establishment of channels, points of contact, best practices, protocols, and/or other mechanisms for coordinating activities related to cybersecurity. This coordination is further potentialized in institutional contexts with clear roles and responsibilities as well as specific intra- and interagency as well as multistakeholder mechanisms.

The coordination envisioned by E-Ciber focuses on **establishing a centralized national governance model** (AE2). The governance model shall focus on promoting the coordination of stakeholders beyond the realm of the FPA; encouraging a joint analysis of key challenges; assisting in de development of public policies; and creating cross-sector discussion groups.

This Strategic Action is perhaps the most concrete one in presenting recommendations. It sets out what could be considered a roadmap outlining the necessary governmental

73 Strategic action 6: Improve cybersecurity legal framework.

74 Strategic action 10: Increase society's maturity level regarding cybersecurity; Strategic action 9: Increase cybersecurity partnerships between the public sector, private sector, the academic community, and society.

75 https://www.codingrights.org/safermanas-dicas-de-seguranca-digital-em-gifs/. https://festival3i.org/mesa/seguranca-digital-para-jornalistas/. https://new.safernet.org.br/content/seguran%C3%A7a-digital#. For international examples, Access Now has developed a digital security helpline available in nine new languages: https://www.accessnow.org/help-pt/.

changes in order to establish a national governance model. These recommendations highlight the need to **establish the GSI as the leading and central actor for "coordinating cybersecurity at the national level." According to the text, this centrality and expansion of scope would enable "a broad, cooperative, participative engagement aligned with cyber defense actions under the responsibility of the Ministry of Defense."**

As previously mentioned, GSI already facilitates and coordinates cybersecurity activities across the FPA. However, the E-Ciber introduces new objectives and expands the scope of action by recommending that the GSI, a relatively small body, takes on the full role in national cybersecurity. Other activities would include creating and coordinating discussion groups in different sectors in order to foment debate "through informal participation mechanisms."

The Strategy also recommends **that a National Cybersecurity Council is established** with the purpose of including various state and non-state actors in "thinking about cybersecurity from a broad, inclusive, modern perspective with an emphasis on concrete national needs." **According to the document, the creation of these groups should also be prescribed in a legislative bill** that would be drafted by the GSI. Through this legal instrument, they would first focus on developing directives for a macro-strategic alignment while also contributing "to increasing the security of organizations and of citizens." [76] However, there are still considerable amounts of uncertainty with regards to the potential impact and benefits of these mechanisms – especially when it comes to enhancing the role and contribution of civil society and the academic community to this debate.

The bill could ideally introduce incentives for consolidating a cybersecurity culture across the country. This would include establishing information sharing protocols, basic principles for national cybersecurity and among other provisions. However, E-Ciber concretely focuses on developing a bill which could establish a National Cybersecurity Law, a National Council, and confirm GSI's role as lead actor in coordinating efforts and policy elaboration in this area.

As well-intentioned as the attempt to establish a cybersecurity law is, the generalized polarization, disinformation, and political instability could place these attempts in check. Confusion regarding concepts associated with cybercrime and disinformation could lead to a reconfiguration of the bill. This is all the more concerning considering what could potentially be included in the regulation of "cybersecurity actions" and in specifying "responsibilities." [77] It is more pressing than ever that politicians understand the distinctions between cybersecurity, cybercrime, cyber defense, and other related terms. The lack of a cybersecurity discussion which is accessible to society may exacerbate misunderstandings regarding which "actions" and "attributions" should or should not be within the scope of the law. This, once again, demonstrates the necessity of public debate as one step towards establishing a cybersecurity culture that integrates operational concerns, policy development and rights protections.

Other challenges to the strategic ambitions of centralized coordination present themselves not only in its form, but also at the institutional level. Countries often appoint a central agency to deal with cybersecurity issues. However, GSI's profile (being largely composed by

76 Cyber Security Summit Brazil. Available at: https://www.youtube.com/watch?v=TUv4wcfb-AY.

77 "Emphasizes the necessity of a law which regulates cybersecurity actions, specifies responsibilities, indicates mechanisms for dialog with society at large, and which allows the Institutional Security Cabinet, along with representatives from all national entities, to exercise its role as strategic, macro coordinator in aligning cybersecurity actions and contributing to the country's evolution in this area in a convergent and structured manner" – extract from E-Ciber.

military) is concerning as it reinforces the preexisting militarization of cybersecurity, while also sidelining diversity in the construction and implementation of coordination activities.

Various questions remain as to how the consultation mechanisms foreseen in the Strategy will foster greater diversity (in terms of sector, gender, race, and discipline) of visions in the consolidation of national cybersecurity governance, and whether this includes effective participation in decision-making processes. Going forward, transparency mechanisms for society to accompany these governance processes (initially) and specific actions (in the future).

While the document highlights the establishment of a centralized model as one of its strategic actions, it fails to provide examples of what this model could be in practice. Australia, Singapore, and the United Kingdom, for example, have opted for a centralized National Cybersecurity Centers. In Australia [78]and the United Kingdom, [79] these centers are integrated into the intelligence system, and are also responsible for incident response activities. Singapore has an agency dedicated specifically to cybersecurity, which is located within its Ministry of Communication and Information. It includes responsibilities that range from incident response to policy development, operations, and representation in international forums.[80]

At the operational level, the Strategy outlines specific recommendations for improving incident response, the protection of critical infrastructure, and information sharing. This includes the development of information sharing mechanisms related to incidents and vulnerabilities and promotion of activities to enhance the interaction between regulatory agencies and critical infrastructure in cybersecurity.

Knowledge Integration

From response activities and incident processing to data protection and the preservation of human rights, security depends not only on articulation between different groups, but also between different forms of knowledge and expertise. This dimension includes activities that range from incident response to data protection and the preservation of human rights. Understanding how other sectors have approached cybersecurity and mapping the initiatives they have developed can help foster new avenues for trust and coordination.

Cybersecurity depends on different kinds of knowledge and expertise. A failure to integrate different visions of threats into the development of policies and technologies can result in the consolidation of a myopic perspective of national risks.[81] Integration depends on mapping national capacities to both effectively understand and respond to emerging threats. Organizations across different sectors already possess significant experience in training and capacity building. Civil society organizations specialized in digital and media rights, for example, have historically worked with different communities, helping them to protect themselves online.

Integration is mentioned in the Strategy's recommendations. It includes: the promotion of exercises and scenarios with organizations from different sectors; incentives for participating in national and international events; and expansion of collaboration in universities, research centers, the private sector, and institutes. However, the concept of knowledge integration across policy and technical divides remains undefined in E-Ciber.

78 https://www.cyber.gov.au/acsc.

79 https://www.ncsc.gov.uk/section/about-ncsc/what-we-do.

80 TER, K.L. Singapore's Cybersecurity Strategy. Computer Law & Security Review, v. 34, p 924-927. 2018.

81 Machmeter, L., Deibert, R., & Lindsay, J. (2020). A Tale of two cybers – how threat reporting by cybersecurity firms systematically underrep resents threats to civil society. Journal of Information Technology & Politics, 1-19, DOI:10.1080/19331681.2020.1776658.

Sustainability of Efforts

The development of mechanisms, partnerships, and activities that can have a long-lasting impact and/or can endure and adapt to changes in the threat and risk landscapes. Sustainability is thus understood in the broad sense, referring to financial sustainability, governance mechanisms, strategies, cooperation mechanisms, transparency and accountability measures, as well as frameworks for monitoring the implementation of activities/objectives.

The sustainability of efforts refers to actions which contribute to a lasting impact in the design of mechanisms, partnerships, and activities. A large proportion of the actions [82] and recommendations included in E-Ciber related to this dimension focus on the adoption of standards that guarantee the continuity and credibility of the systems, networks, and infrastructures. Other recommendations emphasize more practical actions for defining security requirements in cases of remote work and developing cybersecurity solutions for emerging technologies. However, the main requirement for sustainability in nearly all actions recommended by the Strategy depend on the allocation of financial as well as human resources which can meet the demands of coordination, communication, and innovation outlined within the document.

"The main requirement for sustainability in nearly all actions recommended by the Strategy depend on the allocation of financial as well as human resources"

82 Strategic Action 7: Incentivize innovative solutions in cybersecurity; Strategic Action 10: Increase society's cybersecurity maturity level.

E-Ciber's Strengths and Weaknesses

STRENGTHS

- For the first time, a GSI document was submitted for public consultation;
- Recognizes Brazil's international engagement in specialized cybersecurity forums;
- Addresses the development of multistakeholder capacities (National Council, forums, mechanisms for integration between sectors);
- Emphasizes the importance of developing technologies with standards such as privacy and security by default and design;
- Emphasizes the importance of strengthening the role of Brazilian Computer Incident and Response Teams.

WEAKNESSES

- Fails to align expectations related to the E-Ciber. Frustration from various sectors with the strategy's format and lack of clarity regarding what should be accomplished;
- No mention of civil society (or the third sector), only "society" or "society in general";
- Absence of a clear vision for advancing the debate on protocols for information sharing across sectors;
- Communication challenges and lack of trust between GSI and civil society groups;
- Uncertainty regarding GSI's capacity to coordinate such a wide range of activities;
- Lack of clarity with regards to the content to be presented in Cybersecurity Bill;
- Lack a budget (or expectation thereof) for developing national plans and for the implementation of strategic actions.

Conclusions and Recommendations

Despite the challenges outlined in this document, the E-Ciber is an important step towards consolidating both a vocabulary and a strategic vision for Brazil. Faced with criticism regarding E-Ciber's broad character, GSI representatives have argued that its objective is to open the possibility of developing a National Cybersecurity Policy, which will include a National Cybersecurity plan and sectoral plans.[83] The document demonstrates what could be considered the key national interests in advancing cybersecurity as a theme which encompasses all sectors and all of society.

Despite domestic tensions associated with the rising scepticism of the credibility of democratic institutions, the mobilization of the far right, and criticisms to the government for mishandling responses to the Coronavirus crisis, cybersecurity has remained relatively less affected by these political, social and economic challenges. The E-Ciber is an important step for Brazil, although it also unveils a long path ahead before strategic objectives and plans can be fully implemented. Security should not be seen merely as a property of systems, networks, machines, and infrastructure. Cybersecurity is a fundamental component in facing hybrid, 21st-century threats and, as the cyberattacks on the STJ and recent massive data leaks have shown, it is also an important component to preserving democracy and strengthening multistakeholder resilience.

83 De Luca, C. (2020). "Após estratégia, GSI elabora a Política Nacional de Segurança Cibernética". Tilt UOL. Available at: https://porta23.blogosfera.uol.com.br/2020/02/09/apos-estrategia-gsi-elabora-a-politica-nacional-de-seguranca-cibernetica/.

Recommendations

Recommendation 1

Public oversight of the E-Ciber could enhance transparency and accountability in monitoring how strategic objectives are being met. To do so, we recommend the publication of an annual report detailing the achivements and challenges for implementing the E-Ciber.

Recommendation 2

Establish communication channels with civil society and recognize its role as an important actor with experience in training programs. This communication will be fundamental for a more transparent discussion about national cybersecurity and for the inclusion of human rights as a fundamental element in the FPA's cybersecurity agenda.

Recommendation 3

Improve public and private sector information sharing mechanisms related to incidents and vulnerabilities, and establish directives for coordinated vulnerability disclosure. Guides and reports with recommendations from the government on this topic should be accessible to all of society.

Recommendation 4

Although the Strategy includes consultation mechanisms like the Council, its implementation also depends on improving communication between GSI, CSOs and academic groups (from the humanities and from the natural sciences). To this end, it is imperative that GSI construct a communication and outreach to engage more effectively with these groups.

Recommendation 5

Assess GSI's internal capacities vis à vis expanding its roles and responsibilities in national cybersecurity. Future efforts should prioritize multistakeholder implementation plans.

Recommendation 6

Evaluate timing and/or necessity of a Cybersecurity Bill avoiding further confusion between cybersecurity and other themes, such as disinformation.

Annex 1: Strategic Actions and Recommendations

1. Strengthen Cyber governance actions	(1.1) hold governance forums;
	(1.2) create controls for processing restricted information;
	(1.3) establish minimum cybersecurity requirements for public agency contracts;
	(1.4) Implement cyber governance programs and projects;
	(1.5) As well as governance norms stipulated by the Institutional Security Cabinet, adopt globally recognized norms, standards, and models of governance;
	(1.6) Industry should adopt international standards in new product development (privacy/security by design and default);
	(1.7) recommend the adoption of national encryption solutions, as monitored by specific legislation
	(1.8) intensify efforts to combat software piracy
	(1.9) adopt cybersecurity solutions which address integrating initiatives
	(1.10) designate an information security manager
	(1.11) recommend cybersecurity certification in line with international standards
	(1.12) increase use of digital certificates
2. Establish a centralized model of governance on the national level	(2.1) promote coordination among various actors, beyond the federal sphere, in issues related to cybersecurity
	(2.2) promote the joint analysis of challenges faced in combatting cybercrime
	(2.3) assist in public policy formulation
	(2.4) create a national cybersecurity council
	(2.5) create cybersecurity discussion groups in different sectors, all coordinated by the Institutional Security Cabinet, in order to encourage debate on the theme through informal participation mechanisms
	(2.6) establish routine to verify internal cybersecurity compliance in public agencies and private entities
	(2.7) allow for efforts and initiatives to converge and act in a complementary manner in receiving grievance reports, investigating incidents, and promoting awareness and education in society at large. To facilitate implementation, the Institutional Security Cabinet will be responsible for coordinating cybersecurity on the national level, which will allow for broader, cooperative, and participative actions aligned with the cyber defense strategy, as stipulated by the Ministry of Defense

continued

3. Promote a participative, collaborative, credible, and secure environment between the public sector, private secto and society	(3.1) encourage information sharing regarding cyber incidents and vulnerabilities
	(3.2) carry out cyber exercises with multiple actors
	(3.3) establish mechanisms which allow interaction and data sharing on different levels
	(3.4) strengthen the Brazilian Government Response Team for Computer Security Incidents - CTIR Gov, and keep it supplied with personnel and material
	(3.5) emphasize the role of the national Computer Security Incident Response Teams- CSIRTs
	(3.6) improve national infrastructure for investigating cybercrime
	(3.7) encourage the creation and performance of cyber incident response teams - ETIRs, with an emphasis on emerging technologies
	(3.8) release alerts and recommendations
	(3.9) stimulate the use of encryption resources in society wheninformation is considered sensitive
4. Increase level of Government protection	(4.1) include cybersecurity requirements in contracts with government agencies and entities
	(4.2) improve and encourage use of secure communications devices in government
	(4.3) improve and update public sector information systems, infrastructure, and communications systems in line with cybersecurity requirements
	(4.4) recommend that public agencies automatically possess updated and segregated security copies in a protected area
	(4.5) elaborate specific cybersecurity requirements regarding the use of endpoints in public organizations, understood here as equipment connected to a terminal or some network or communication system
	(4.6) in cybersecurity policies, include requirements related to managing the supply chain
	(4.7) include cybersecurity requirements in privatization processes related to essential services
	(4.8) monitor the implementation of minimum cybersecurity requirements for service providers in the supply chain
5. Increase protection of Critical National Infrastructure	(5.1) promote interaction between regulatory agencies for critical infrastructure in addressing cybersecurity issues
	(5.2) encourage the adoption of cybersecurity activities for critical infrastructure
	(5.3) encourage organizations to implement cybersecurity policies which include, among other aspects, metrics, assessment mechanisms, and periodic revisions.
	(5.4) incentivize the creation of ETIRs
	(5.5) encourage critical infrastructure to notify CTIR Gov regarding cyber incidents
	(5.6) encourage the participation of critical infrastructure in cyber exercises

continued

6. Improve the cybersecurity legal framework	(6.1) identify and address issues not covered by existing legislation
	(6.2) carry out efforts in order to include new cybercrime categories in Decree n. 2.848, of 7 December 1940 - Penal Code
	(6.3) elaborate norms for emerging technologies
	(6.4) create incentive policies for hiring specialized cybersecurity work
	(6.5) define cybersecurity requirements for remote work programs
	(6.6) With coordination from the Institutional Security Cabinet, elaborate a potential bill on cybercrime, with directives that provide an aligned macro-strategy for the sector and which decisively contributes to increasing the security of organizations and citizens in general.
7. Incentivize innovative solutions in cybersecurity	(7.1) propose the inclusion of cybersecurity in research promotion programs
	(7.2) encourage the creation of cybersecurity research and development programs in the federal Executive branch and in the private sector
	(7.3) facilitate research investment through public and private funds
	(7.4) create incentive programs for developing cybersecurity solutions
	(7.5) encourage the creation of cybersecurity startups
	(7.6) stimulate development and innovation for cybersecurity solutions in emerging technologies
	(7.7) encourage the adoption of global technology standards which allow for international interoperability
	(7.8) encourage the development of encryption skills and solutions
	(7.9) stimulate continued research into the use of spectral intelligence
	(7.10) establish minimum cybersecurity requirements which guarantee the full, responsible, and secure potential of fifth generation mobile network technology - 5G
8. Increase Brazil's international cybersecurity cooperation	(8.1) stimulate international cybersecurity cooperation
	(8.2) encourage cybersecurity discussions in international agencies, forums, and groups in which Brazil is a member
	(8.3) increase international relations with Latin American countries
	(8.4) promote international cybersecurity events and exercises
	(8.5) participate in international events within the country's interest
	(8.6) increase cybersecurity cooperation accords
	(8.7) increase the use of international mechanisms in combatting cybercrime
	(8.8) stimulate national participation in future initiatives for structuring norms, as well as those related to the creation of security standards for emerging technologies
	(8.9) identify, encourage, and take advantage of new commercial opportunities in cybersecurity

continued

9. Increase cybersecurity partnerships between the public sector, private sector, academic community, and society in general	(9.1) increase cooperation between the government, the academic community, and private initiatives in promoting and implementing E-Ciber
	(9.2) maintain a collaborative environment which allows for the study and ample utilization of emerging technologies
	(9.3) establish partnerships to encourage the private sector to invest in cybersecurity measures
	(9.4) encourage meetings with important cybersecurity actors
	(9.5) if necessary, stimulate the creation of cybersecurity working groups and forums
	(9.6) encourage the creation of information sharing mechanisms related to cyber risks
	(9.7) create partnerships between the federal government, the states, the Federal District, municipalities, the Public Prosecutor's office and the academic community for implementing cybersecurity programs, projects, and activities which reach society as a whole
10. Increase society's cybersecurity maturity level	(10.1) encourage public agencies and private businesses to carry out internal awareness campaigns
	(10.2) carry out general awareness activities
	(10.3) create public policies that promote society's awareness of cybersecurity
	(10.4) propose the inclusion of cybersecurity, its basic skillset, and the ethical use of information in early childhood education, middle school, and high school
	(10.5) encourage the creation of advanced courses in cybersecurity
	(10.6) propose the creation of incentive programs for undergraduate and graduate cybersecurity programs in Brazil and abroad
	(10.7) promote cybersecurity research and development
	(10.8) create continuing education programs for professionals in the public and private sectors
	(10.9) encourage professional education for combatting cybercrime
	(10.10) produce cybersecurity training events
	(10.11) encourage participation in national and international cybersecurity events
	(10.12) improve mechanisms for integration, collaboration, and incentives between universities, institutes, research centers, and the private sector in the field of cybersecurity
	(10.13) encourage cybersecurity simulation exercises
	(10.14) promote cybersecurity knowledge management while coordinating with key figures in the field in order to optimize the identification, selection, and employment of talented individuals

Also read

PUBLICATION

REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO: avaliação de experiências internacionais

Louise Marie Hurel, Mariana Marques Rielli e Pedro Augusto P. Francisco

(June 2020)

STRATEGIC NOTE 30

A STRATEGY FOR CYBERSECURITY GOVERNANCE IN BRAZIL

Louise Marie Hurel and Luisa Cruz Lobato

(September 2018)

STRATEGIC PAPER 11

DECONSTRUCTING CYBER SECURITY IN BRAZIL: THREATS AND RESPONSES

Gustavo Diniz, Robert Muggah and Misha Glenny

(December 2014)

IGARAPÉ INSTITUTE
a think and do tank

The Igarapé Institute is an independent think and do tank, dedicated to integrating security, development, and climate agendas. The Institute's goal is to propose data-driven solutions and partnerships to global challenges through research, new technologies, and strategic communication. The Institute is a nonprofit, independent and non-partisan institution based in Rio de Janeiro, active in Brazil and across Latin America and Africa. The Institute was ranked the world's best social policy think tank in 2019 by Prospect Magazine, and has been listed among the top 100 Brazilians NGOs since 2018.

Supported by:

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Instituto Igarapé

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Layout
Stephanie Gonçalves

Direção criativa
Raphael Durão - STORMdesign.com.br

ISSN 2359-0998

www.igarape.org.br

IGARAPÉ INSTITUTE
a think and do tank