CONTEMPORARY BRAZIL

Invited article. Associate Editor: Marco Antonio Teixeira
Versão original | DOI: https://doi.org/10.12660/cgpc.v29.90972

WHAT IS THE FUTURE OF BRAZIL'S CYBERSECURITY GOVERNANCE?

Qual é o futuro da governança de cibersegurança no Brasil?

¿Cuál es el futuro de la gobernanza de ciberseguridad de Brasil?

Luiz Rogério Franco Goldoni *[1,2] | luizrfgoldoni@gmail.com | ORCID: 0000-0001-5257-9470
Karina Furtado Rodrigues[1,3] | karinafrodrigues@gmail.com | ORCID: 0000-0001-9330-6399
Breno Pauli Medeiros[1,2,4] | breno.pauli@gmail.com | ORCID: 0000-0002-9839-5252

*Corresponding author
[1]Escola de Comando e Estado-Maior do Exército, Programa de Pós-Graduação em Ciências Militares, Rio de Janeiro, RJ, Brazil
[2]Laboratório de Poder Cibernético, Rio de Janeiro, RJ, Brasil
[3]Laboratório de Governança, Gestão e Políticas Públicas em Defesa Nacional, Rio de Janeiro, RJ, Brazil
[4]Centro de Tecnologia e Sociedade, Fundação Getúlio Vargas, Rio de Janeiro, RJ, Brazil

ABSTRACT

In 2023, Brazil enacted its first national cybersecurity policy. The policy emerged as a response to worrisome diagnoses, which listed information security and cybersecurity among Brazil's public administration high-risk vulnerabilities, according to a 2022 report from the Federal Court of Auditors. What lies ahead for Brazil's newly enacted Cybersecurity National Policy? Our analysis aims to answer this question by unraveling the existing cyber governance structure that the new policy inherited and by analyzing the governance structure debated and enacted by the current policy. We conclude that Brazil has made several efforts to securitize cyberspace through a broad but disconnected collection of documents; their implementation maturity is unclear, and the Cybersecurity National Policy fails to design straightforward policy tools to address those challenges.

Keywords: governance, cybersecurity, Brazil, public policy analysis, PNCiber.

RESUMO

Em 2023, o Brasil promulgou sua primeira política nacional de cibersegurança. Esta surgiu como resposta a diagnósticos preocupantes, que colocam a segurança da informação e a cibersegurança entre as vulnerabilidades de alto risco da administração pública brasileira, segundo relatório de 2022 do Tribunal de Contas da União (TCU). O que está por vir para a recém-promulgada Política Nacional de Cibersegurança (PNCiber) do Brasil? Nossa análise visa responder a essa pergunta, primeiro desvendando a estrutura de governança cibernética existente que a nova política herdou e, segundo, analisando a estrutura de governança debatida e promulgada pela política atual. Conclui-se que o Brasil fez diversos esforços para securitizar o ciberespaço por meio de uma coleção ampla, porém desconexa, de documentos, cuja maturidade de implementação não está clara, sem que a PNCiber forneça ferramentas de políticas públicas diretas para enfrentar esses desafios.

Palavras-chave: *governança, cibersegurança, Brasil, análise de políticas públicas, PNCiber.*

RESUMEN

En 2023, Brasil promulgó su primera política nacional de ciberseguridad. Esta surgió como respuesta a diagnósticos preocupantes, que sitúan la seguridad de la información y la ciberseguridad entre las vulnerabilidades de alto riesgo de la administración pública brasileña, según un informe de 2022 del Tribunal Federal de Cuentas. ¿Qué depara el futuro para la recién promulgada Política Nacional de Ciberseguridad de Brasil? Nuestro análisis busca responder a esta pregunta, primero desentrañando la estructura de gobernanza cibernética existente que la nueva política heredó y, segundo, analizando la estructura de gobernanza debatida y promulgada por la política actual. El desafío es que Brasil ha realizado varios esfuerzos para resguardar el ciberespacio a través de una amplia pero desconectada colección de documentos, cuya madurez de implementación no está clara, y la Política Nacional de Ciberseguridad (PNCiber) no logra diseñar herramientas de políticas públicas directas para abordar esos desafíos.

Palabras-clave: *gobernanza, ciberseguridad, Brasil, análisis de políticas públicas, PNCiber.*

INTRODUCTION

What lies ahead for Brazil's newly enacted Cybersecurity Policy? Brazil's efforts to secure cyberspace reached a milestone in 2023 with the enactment of the National Cybersecurity Policy (PNCiber), marked by the presidential decree nº 11.856 (2023). The decree establishes cybersecurity goals and creates a national cybersecurity committee (CNCiber) in which representatives of distinct sectors of society can develop subsequent policy programs and strategies.

The decree emerged as a response to a worrisome diagnosis. According to a 2022 report from Brazil's Federal Court of Auditors (Tribunal de Contas da União, 2022), information security and cybersecurity are high-risk vulnerabilities for the country's public administration. The report reveals that 73.1% of federal government services rely entirely on digital platforms, with 83.7% partially relying on them. Moreover, 74.6% of public organizations lack established backup policies, and among those with such policies, 66% do not encrypt their data. The TCU emphasizes that current Brazilian legislation does not allocate authorities or resources to regulate cyberspace. The report highlights recent cyber incidents in Conecte-SUS, the Superior Tribunal of Justice, and the Federal Comptroller General. Overall, the TCU concludes that the federal government and the broader public sector lack sufficient preparation and empowerment to protect public assets in cyberspace.

The PNCiber is not the only effort to secure cyberspace in the country. Since the early 2000s, significant strides have been taken regarding cyber policies. Between 2018 and 2020, two crucial norms were established: the National Information Security Policy (PNSI, decree nº 9.637, 2018) and the National Cyber Security Strategy (E-Ciber, decree nº 10.222, 2020). These initiatives envisaged a single actor coordinating and managing national cybersecurity structures: the Institutional Security Office of the Republic's Presidency (GSI).

These and other norms established a governance structure overlooked by most Brazilian public administration scholars. Evidence of that is the absence of articles using the keyword "cybersecurity" in Brazil's most prestigious Public Administration journals, such as *Cadernos Gestão Pública e Cidadania*, *Revista de Administração Pública*, and *Administração Pública e Gestão Social*.

Interestingly, Cyber policies are a perfect fit for a governance perspective in which it is crucial to have institutional arrangements directed to solve public problems in a context where responsibility frontiers are blurred, a plurality of autonomous actors are needed, both from inside and outside the state, and when the best role governments can play is to steer and guide (Milward & Provan, 2000; Peci et al., 2008; Stoker, 1998).

Accordingly, these governance arrangements should be able to effectively set goals, assign responsibilities, and improve the overall performance of this network of actors and policies. Despite the abundance of norms in Brazil, they are disconnected and with uncertain implementation maturity. The agency responsible for creating and monitoring their implementation, the GSI, does not have enough capacity to do it alone (Goldoni et al., 2023), often relying on the Brazilian Army's capacity to undertake some of its activities. The newly enacted policy also does not count on more financial and workforce resources to make it happen, at least for now.

We set two secondary goals to understand the future of cybersecurity governance in Brazil: (i) to draw the existing cybersecurity governance from the norms the new policy is inheriting; (ii) to assess the challenges posed by the current policy to existing issues, considering the notable disparities between the cyber policy draft introduced in the first half of 2023 and the subsequently enacted decree. Therefore, the following section makes the case of governance being crucial to cybersecurity; the third section delves into Brazil's cybersecurity governance structure; the fourth section discusses the intents and limits of the current Brazilian Cybersecurity Policy compared to the draft bill presented months before the policy enactment; and the fifth section presents our final considerations.

WHY A GOVERNANCE APPROACH TO CYBERSECURITY IS CRUCIAL

Governance is a polysemous term that can receive many adjectives, such as collaborative, asymmetric, network, participatory, and so on (Ansell & Torfing, 2022; Buta & Teixeira, 2020; Calmon & Costa, 2013). In this article, we consider public governance as a public administration paradigm, where governance usually encompasses decision-making processes involving public and private actors in a combined effort to provide services or solve specific public problems. This understanding aligns with Stoker's (1998) definition, which is composed of five 'propositions':

1. Governance refers to a set of institutions and actors drawn from and beyond government.
2. Governance identifies the blurring of boundaries and responsibilities for tackling social and economic issues.
3. Governance identifies the power dependence in the relationships between institutions involved in collective action.
4. Governance is about autonomous self-governing networks of actors.
5. Governance recognizes the capacity to get things done, which does not rest on the power of government to command or use its authority. It sees the government as being able to use new tools and techniques to steer and guide (p. 16).

After that, the key to governance is mobilizing a plurality of actors to deal with the complexity of social problems, which can involve many agencies, whether from the state or a mix of public and private entities. In this sense, this problem-solving institutional arrangement is a perfect fit for cybersecurity policies. Let us explore why.

A country's cybersecurity lies in the security of an enormous number of actors that, if disconnected, have increased vulnerabilities. State actors comprise all state agencies that provide social services that, if paralyzed, can compromise critical public policy. Private companies also play a vital role in a country's cybersecurity, especially those considered 'critical infrastructure' ones.

Consequently, the regulatory agencies of critical infrastructure sectors play an essential role in creating and demanding cybersecurity measures from companies and offering them support in the case of cyberattacks. If a company or an agency is attacked, it should be able to identify and respond to the attack. However, neither agencies nor companies often have enough resources to maintain highly trained IT personnel. That is when knowing who can help and who to inform of the attack is paramount. Additionally, if attacks are being orchestrated in many agencies and companies, reporting tools can be even more critical in identifying and neutralizing them.

In conclusion, if the policy sees digital services, governmental information systems, agencies, and companies compartmentalized, not taking governance seriously, a wide array of vulnerabilities will persist, with higher impacts due to poor cyber resilience (Linkov & Kott, 2019). Cyber policies should consider all five of Stoker's principles of what composes governance.

PNCIBER'S INHERITED CYBERSECURITY GOVERNANCE STRUCTURE

Contemporary efforts to protect Brazilian cyberspace date back to 2008, when cyber defense was first considered a strategic sector in the National Defense Strategy. This was followed by the Cybersecurity Green Book published in 2010, which established the groundwork for developing a National Cybersecurity Policy (Hurel, 2021).

The following decade saw the development of the Cyber Crime Law, Law n. 12.737 (2012) against computer invasion and tampering, complemented by Law n. 12.735 (2012), which created specialized police to address digital crimes. These were followed by the *Marco Civil* (Law n. 12.965, 2014) and the General Personal Data Protection Law (LGPD, Law n. 13.709, 2018), which served as legislative cornerstones for individual rights and online data protection and privacy.

More recent efforts to digitalize Brazilian public administration have included the publication of three national policies: the Strategy for Digital Transformation (E-Digital, Decree n. 9.319, 2018), the Decree for Governance and Data Sharing (Decree n. 10.046, 2019), and the Digital Governance Policy (Decree n. 8.638, 2016). The latter was replaced in 2020 by the Digital Government Strategy for 2020-2022 (Decree n. 10.332, 2020).

The E-Digital strategy is particularly relevant for our analysis. Formulated by the Ministry of Science, Technology, Innovation, and Communications, it proposes best practices for critical infrastructure and cyberspace. This emphasis on protecting critical infrastructure was further detailed through the National Policy for Critical Infrastructure Safety (PNSIC, Decree n. 9.573, 2018), the National Strategy for Critical Infrastructure Safety (ENSIC, Decree n. 10.569, 2020), and the National Plan for Critical Infrastructure Safety (PLANSIC, Decree n. 11.200, 2022). These documents provided general guidelines for safeguarding critical infrastructure.

Cyber risks are briefly acknowledged by ENSIC's strategic objective to "[e]ncourage the adoption of resources and procedures aimed at cybersecurity in critical infrastructures" (Decree n. 10.569, 2020, p. 9, our translation). Additionally, PLANSIC acknowledges that it must be

following the (Decree n. 10.222, 2020) National Strategy for Cyber Security (E-CIBER) and the (Decree n.10.748, 2021) Federal Network of Cyber Incident Management (ReGIC), which are both investigated in our analysis.

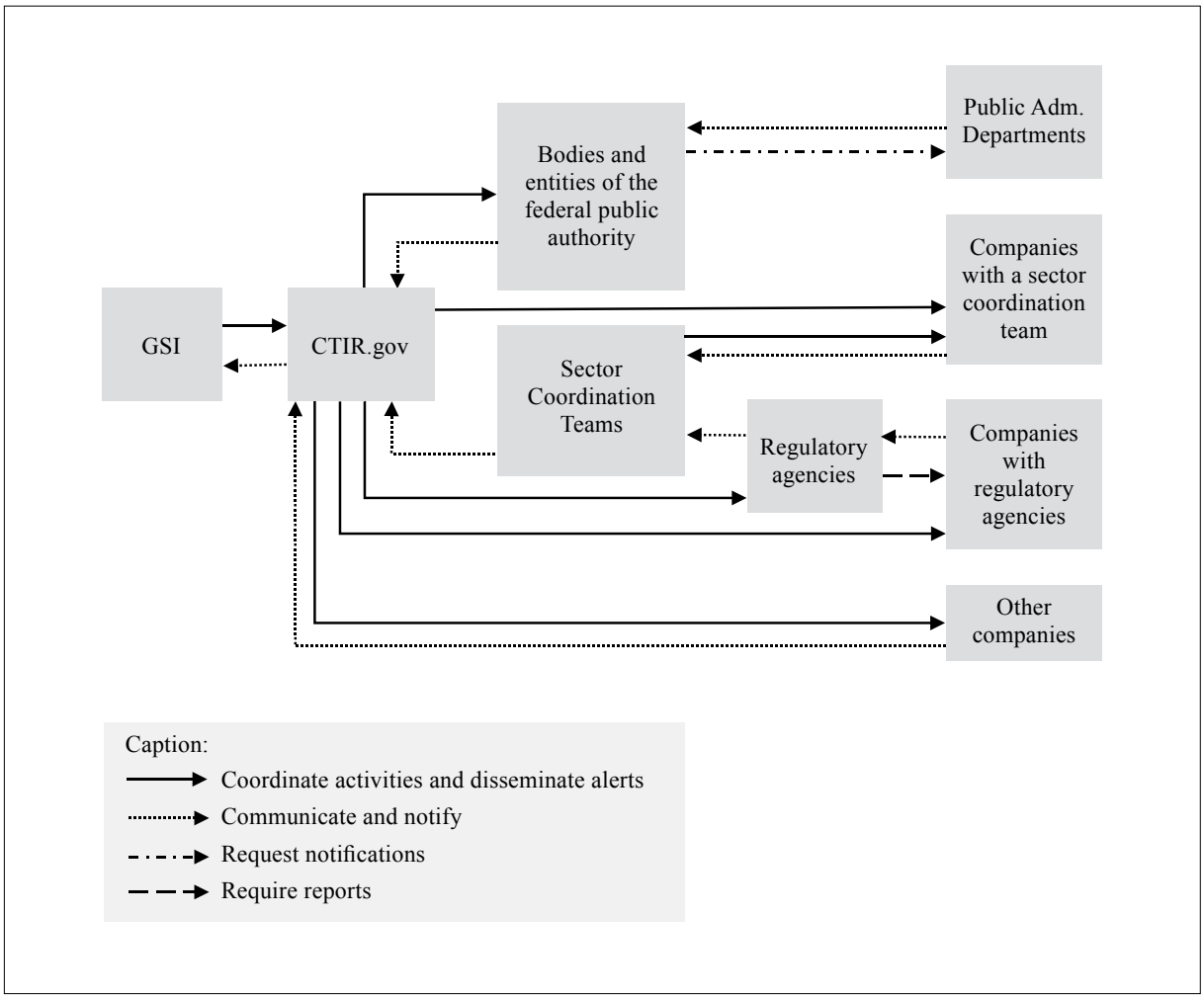
This regulatory structure, comprising policy, strategy, and plan, is replicated in cyber-specific documents within Brazil. The National Policy for Information Security (PNSI), a cornerstone of the country's cyber governance, was initially released in 2018 and updated in 2021. The PNSI broadly defines information security as cybersecurity, cyber defense, physical data safety, and information confidentiality, integrity, and availability assurance. Aligned with the E-Digital strategy, it emphasizes the necessity for a national cybersecurity policy spanning both public and private sectors.

The PNSI emphasizes coordination across various institutions, adopting a top-down approach with GSI leading information security efforts. It anticipates the development of a National Strategy for Information Security (ENSI) with modules covering cybersecurity, cyber defense, critical infrastructure safety, confidential information security, and protection against data leaks. However, only the National Cybersecurity Strategy (E-Ciber), valid until 2023, was published.

The PNSI mandates the Defence Ministry's role in supporting GSI for cybersecurity, acknowledging the intersection between cybersecurity and cyber defense. In its 2021 updated version (Decree n. 10.641, 2021), the PNSI requires federal entities to establish Cyber Incident Response teams coordinated by CTIR.gov, part of a broader incident response network. This evolution led to the Federal Network of Cyber Incident Management (ReGIC) creation in 2021 (Decree n. 10.748, 2021), aimed at enhancing coordination among federal bodies for preventing, treating, and responding to cyber incidents. ReGIC mandates admission for public administration entities, with a 12-month deadline for full directive implementation.

While the term "governance" is absent in ReGIC documentation, it details how to respond to cyber incidents, requiring public agencies to report to sector coordination teams or directly to CTIR.gov. ReGIC's network design outlines incident response procedures and specifies sectors requiring coordination teams. Article 11 mandates CTIR.gov to coordinate the cyber incident efforts of ReGIC's members, while Article 12 assigns teams the responsibility of reporting vulnerabilities and incidents affecting national critical infrastructure. This establishes a top-down network governance, depicted in Figure 1.

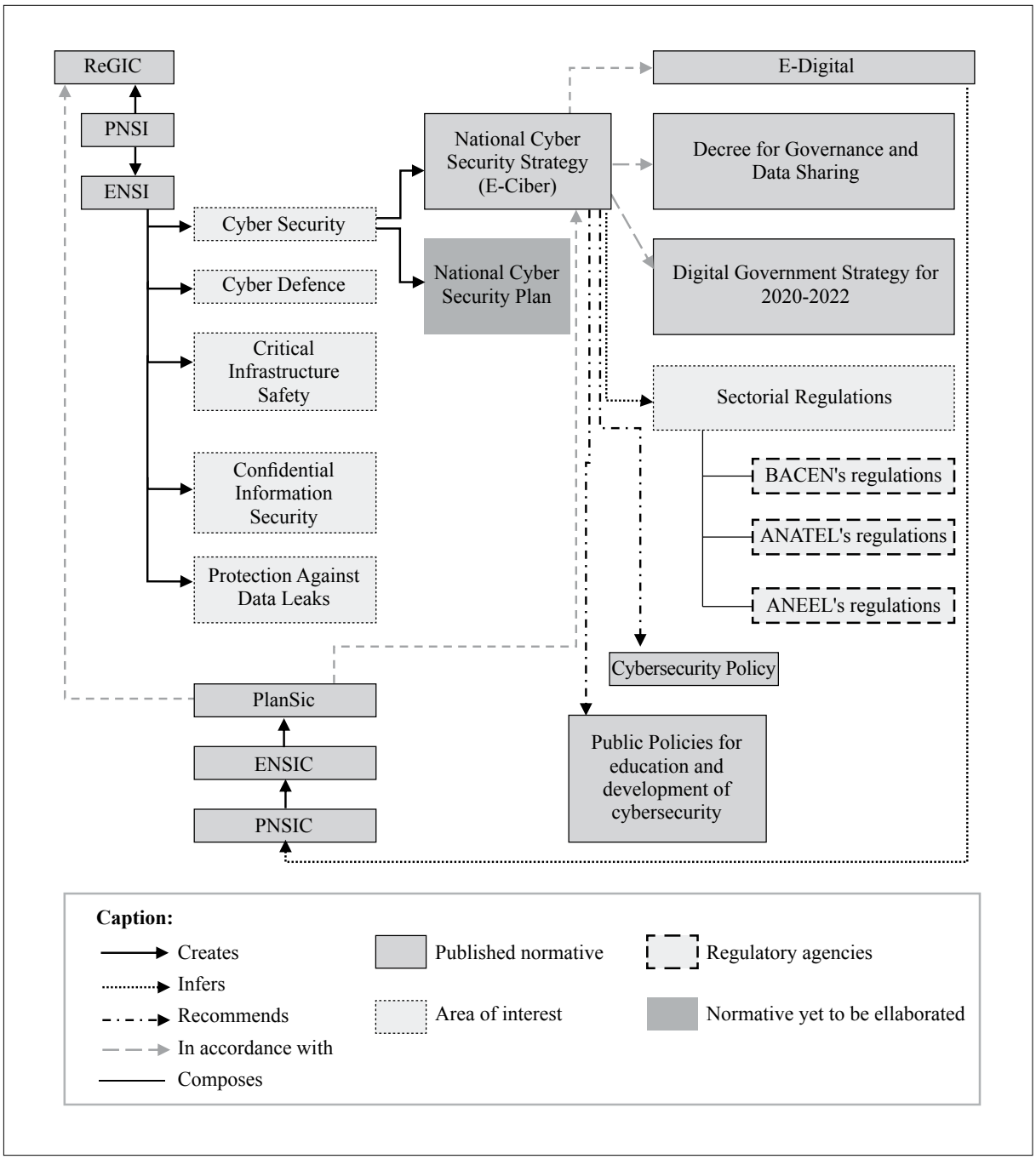
Figure 1 – ReGIC Governance Structure



Source: Adapted from ReGIC (Decree n. 10.748, 2021).

The overlapping frameworks underpinned by these different policies and strategies create a complex interaction and network governance system in Brazil's cyberspace. These relationships are mapped below (Figure 2).

Figure 2 – The Relationship between E-governance and Information Security Documentation



At the sectoral level, and mirroring ReGIC's requirements, the Regulatory Agency of Telecommunications (ANATEL) (Article 9 of its resolution) regulates that notification of the most relevant cyber incidents must occur horizontally, between members and companies from

respective sectors, as well as vertically, to regulatory agencies (Resolution n. 740, 2020). The Regulatory Agency on Electric Energy (ANEEL) must be notified of the most relevant cyber incidents, but it omits mention of horizontal notification (Normative Resolution Aneel n. 964, 2021).

While E-Ciber recommends sectoral regulations, ReGIC establishes sectoral plans for cyber incident management. These are mandatory and should be developed by sectoral coordination teams. Under ReGIC (Article 13), GSI is supposed to disclose the periodicity and essential elements of these plans. Its 2022 Sectoral Plan establishes directives for the other sectoral plans (Edict GSI/PR n. 120, 2022). Despite the implementation of sectoral regulations conducted by some regulatory agencies, such as the Central Bank of Brazil (BACEN), ANATEL, and ANEEL, this process has not been fully completed in all sectors and agencies.

PNCIBER'S PROMISES AND REALITY

In this section, we aim to understand what the PNCiber adds to the former cyber governance, knowing that there are huge differences between what the GSI presented in May 2023 in a draft bill and the policy decree enacted on December 26, 2023.

The May 2023 draft bill

The May 2023 draft bill published by the GSI envisioned the creation of the National Cybersecurity Policy (PNCiber). The document was extensive and addressed the establishment of a National Cybersecurity Policy, the creation of the National Cybersecurity Agency (ANCiber), the National Cybersecurity Committee (CNCiber), and the Cabinet of Cybercrisis Management (Gabinete de Segurança Insitucional, 2023).

Four of the 45 pages of the draft bill were dedicated to a "Presentation" and six to an "Exposition of Motives," where national vulnerabilities related to cybersecurity were listed, motivated by various international and national rankings and studies that highlighted the risks and damages cyber incidents already caused to the Brazilian economy. The goal was to justify the necessary investments to create ANCiber, deemed by the draft bill as essential for achieving the policy's objectives.

The draft also stated that one policy goal (GSI, 2023) was to "unify the existing regulatory 'patchwork' in the country" (p. 1). However, careful reading of the document may indicate otherwise. This is because the document does not mention the PNSIC or the PNSI at any time, and the E-Ciber only appears in a few paragraphs of the second page of the "Exposition of Motives." The ReGIC is only mentioned by name in the middle of the document, without any emphasis. This might point to inefficiency or substitutivity of the old norms and structures or, worse, that they were "dead letter legislation."

The policy objectives listed in the draft bill are broad and ambitious. However, the document does not mention how they would be achieved. It only refers to a future national cybersecurity strategy, a national cybersecurity plan, and the ANCiber.

Furthermore, as Goldoni et al. (2023) state, the document is silent on how ANCiber would relate to the existing regulatory agencies. "Would there be a suppression of competencies in the other agencies? Would the ANCiber regulate the other regulatory agencies? Could they be held accountable by ANCiber?" (Goldoni et al., 2023). Additionally, we wonder how ANCiber would be funded.

The answers to these questions are vital for a glimpse into which future governance can take place. Mainly because the agency seemed to be the gravitational force of the draft bill and, if created, would be staffed by 800 new public servants and through the creation of 300 commissioned positions in a job market that lacks personnel and with difficult employee retention, which would require high salaries. It is unknown how much the difficulty of financing such an endeavor contributed to the absence of any mentions of the ANCiber in the publication of the PNCiber in December 2023.

The policy enacted by Decree n. 11.856 (2023)

The enacted policy is way shorter than the draft bill, totaling approximately four pages. It was signed by President Lula on December 26, 2023, through Decree n. 11.856 (2023). Its publication via a decree rather than a bill suggests that the subject did not gain the proper relevance in the National Congress. It also did not establish the creation of the highly expected cybersecurity agency.

Regarding policy objectives, little but significant changes occurred, as seen in Chart 4. The removal of promoting the "ethical use of cyber activities and associated technologies in the country" (objective VII of the draft) and the inclusion of developing "regulation, oversight, and control mechanisms aimed at enhancing national cybersecurity" (objective X of the published policy) stands out. At this point, subjective goals were substituted for more concrete ones (regulation and control mechanisms).

Chart 4 – PNCiber's Objectives

POLICY OBJECTIVES IN GSI'S DRAFT BILL	POLICY OBJECTIVES IN DECREE N. 11.856 (2023)
I - guarantee the confidentiality, integrity, authenticity, and availability of cyber assets of interest to Brazilian society.	I - promote the development of national products, services, and technologies aimed at cybersecurity.
II - promote cyber-protection and cyber-resilience of the Public Power, of cyber-assets of interest, and of society as a whole	II - ensure the confidentiality, integrity, authenticity, and availability of solutions and data used for the processing, storage, and electronic or digital transmission of information
III - develop a cybersecurity culture in Brazilian society	III - strengthen diligent action in cyberspace, especially among children, adolescents, and the elderly

(continua)

(conclusão)

Chart 4 – PNCiber's Objectives

POLICY OBJECTIVES IN GSI'S DRAFT BILL	POLICY OBJECTIVES IN DECREE N. 11.856 (2023)
IV - encourage the coordination of the exchange of cybersecurity information between: a) government spheres; b) the private sector; and c) society in general	IV - contribute to combating cybercrime and other malicious actions in cyberspace
V - promote productive and technological autonomy in the field of cybersecurity	V - encourage the adoption of cyber protection and risk management measures to prevent, avoid, mitigate, reduce, and neutralize vulnerabilities, incidents, and cyber-attacks and their impacts
VI - promote Brazil's participation in the global supply chain of products and services related to cybersecurity.	VI - enhance the resilience of public and private organizations to incidents and cyber-attacks.
VII - promote the ethical use of cyber assets and its associated technologies in the country	VII - develop education and technical-professional training in cybersecurity within society
VIII - promote the fight against cybercrime	VIII - promote scientific research, technological development, and innovation activities related to cybersecurity
IX - promote actions that contribute to the security and stability of the global digital environment	IX - enhance coordinated efforts and the exchange of cybersecurity information among: a) the Union, States, the Federal District, and Municipalities; b) the Executive, Legislative, and Judicial branches; c) the private sector; and d) society in general
X - increase Brazil's international projection and engage the country in international decision-making processes to uphold national values and interests.	X - develop regulatory, oversight, and control mechanisms aimed at improving national cyber security and resilience
	XI - implement collaboration strategies to develop international cooperation in cybersecurity

Source: Decree n. 11.856 (2023) and GSI (2023, p. 14).

Furthermore, the published policy broke down and developed objectives previously presented in the draft: Objective I of the Policy encompasses objectives V and VI of the draft, while objectives III and VII of the PNCiber develop the ideas contained in objective III of the draft. Another notable example was the change in wording of objective X of the draft, which became represented by objective XI of the policy.

Like the draft, the PNCiber indicates that it will be up to the National Cybersecurity Strategy and the National Cybersecurity Plan (instruments of the PNCiber) to implement these goals. However, it remains silent on how and when these mechanisms will be created and established.

Also, the document infers that the instituted National Cybersecurity Committee (CNCiber) would be responsible for implementing and updating the PNCiber and its instruments.

The importance of the CNCiber can be measured by the space dedicated to it in the text of Decree 11.856 of December 26, 2023: almost two-thirds. On January 11, 2024, the GSI made a public call to fill vacancies in the CNCiber, related to representatives of civil society, scientific, technological, and innovation institutions, and the business sector. On February 9, 2024, GSI Ordinance No. 6 designated all Committee members.

FINAL CONSIDERATIONS

Brazil has developed myriad legislation regarding its cyberspace, although disconnectedly and with an unclear implementation. Not all agencies adhered to the ReGIC, and not all critical infrastructure sectors elaborated and implemented cybersecurity sectoral norms, with a high heterogeneity among them. In this context, the promise of a national cybersecurity policy emerges with the GSI's draft bill proposal.

Despite its aspirations, the policy was only a shred of what it was first thought to be. What remained was the structure of policy objectives and the creation of the CNCiber. Will existing governance mechanisms persist? Will CNCiber propose to reform Brazil's norms on the subject? With few or no mention of most previous norms, such as E-Ciber, ReGIC, and others, these policy steps remain to be seen.

Since the policy is overly comprehensive, there are too few clues about what will be done and which paths the elaboration of the National Cybersecurity Strategy and Plan will take. Furthermore, we do not know if the ANCiber—the gravitational center of the policy's first proposal—will be created since PNCiber is silent in this respect.

Similarly, only the future will tell what the CNCiber's actual role will be: a committee that proposes and advises on public policies or an entity that simply endorses what the GSI thinks and proposes. Given the historical background previously reported here, we can only hope it is the former.

REFERENCES

Ansell, C., & Torfing, J. (Eds.). (2022). *Handbook on theories of governance*. Edward Elgar Publishing.

Buta, B. O., & Teixeira, M. A. C. (2020). Governança pública em três dimensões: Conceitual, mensural e democrática. *Organizações & Sociedade*, 27(94), 370-395. https://doi.org/10.1590/S1984-92302008000300002

Calmon, P., & Costa, A. T. M. (2013). Redes e governança das políticas públicas. *RP3-Revista de Pesquisa em Políticas Públicas*, (1), 1-29. https://periodicos.unb.br/index.php/rp3/article/view/11989

Decreto n. 8.638, de 15 de janeiro de 2016. (2016). Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Brasília, DF.

Decreto n. 9.203, de 22 de novembro de 2017. (2017). Dispõe sobre a Política de Governança da Administração Pública Federal direta, autárquica e fundacional. Brasília, DF.

Decreto n. 9.319, de 21 de março de 2018. (2018). Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Brasília, DF.

Decreto n. 9.573, de 22 de novembro de 2018. (2018). Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, DF.

Decreto n. 9.637, de 26 de dezembro de 2018. (2018). Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto n. 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF.

Decreto n. 10.046, de 9 de outubro de 2019. (2019). Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, DF.

Decreto n. 10.222, de 5 de fevereiro de 2020. (2020). Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, DF.

Decreto n. 10.332, de 28 de abril de 2020. (2020). Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília, DF.

Decreto n. 10.569, de 9 de dezembro de 2020. (2020). Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF.

Decreto n. 10.641, de 2 de março de 2021. (2021). Altera o Decreto n. 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, DF.

Decreto n. 10.748, de 16 de julho de 2021. (2021). Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Brasília, DF.

Decreto n. 11.200, de 15 de setembro de 2022. (2022). Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Brasília, DF.

Decreto n. 11.856 de 26 de dezembro de 2023. (2023). Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Brasília, DF.

Goldoni, L., Rodrigues, K. & Oliveira, T., Jr. (2023, June 8). O urgente debate sobre a proposta de Política Nacional de Cibersegurança. *Estadão*. https://www.estadao.com.br/

Gabinete de Segurança Institucional da Presidência da República. (2022). *Portaria gsi/pr nº 120, de 21 de dezembro de 2022*. https://in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918

Gabinete de Segurança Institucional da Presidência da República. (2023). *PNCiber – Apresentação do projeto*. https://www.gov.br/gsi/pt-br/ssic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf

Hurel, L. M. (2021). *Cibersegurança no Brasil: Uma análise da estratégia nacional*. Instituto Igarapé. https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf

Lei n. 12.735, de 30 de novembro de 2012. (2012). Altera o Decree-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal, o Decree-Lei n. 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF.

Lei n. 12.737, de 30 de novembro de 2012. (2012). Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF.

Lei n. 12.965, de 23 de abril de 2014. (2014). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF.

Lei n. 13.709, de 14 de agosto de 2018. (2018). Dispõe sobre Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF.

Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks (Vol. 1). New York, NY: Springer International Publishing.

Milward, H. B., & Provan, K. G. (2000). Governing the hollow state. *Journal of Public Administration Research and Theory*, *10*(2), 359-380. https://doi.org/10.1093/oxfordjournals.jpart.a024273

Peci, A., Pieranti, O. P., & Rodrigues, S. (2008). Governança e New Public Management: Convergências e contradições no contexto brasileiro. *Organizações & Sociedade*, *15*, 39-55. https://doi.org/10.1590/S1984-92302008000300002

Portaria GSI/PR n. 120, de 21 de dezembro de 2022. (2022). Aprova o Plano de Gestão de Incidentes cibernéticos para a administração pública federal. Brasília, DF.

Resolução n. 740, de 21 de dezembro de 2020. (2020). Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Brasília, DF.

Resolução Normativa Aneel n. 964, de 14 de dezembro de 2021. (2021). Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Brasília, DF.

Stoker, G. (1998). Governance as theory: Five propositions. *International Social Science Journal*, *50*(155), 17-28. https://doi.org/10.1111/1468-2451.00106

Tribunal de Contas da União. (2022). *Lista de alto risco da administração pública federal: Segurança da informação e segurança cibernética*. Brasília, DF. https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html

NOTE

This work was supported by Fundação Carlos Chagas de Amparo à Pesquisa do Estado do Rio de Janeiro - Programa Jovem Cientista do Nosso Estado [E-26/201.423/2022]

CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare.

AUTHORS' CONTRIBUTION

Luiz Rogério Franco Goldoni: Conceptualization; Data curation; Formal analysis; Investigation; Project administration; Supervision; Validation; Visualization ; Writing – original draft; Writing – proofreading, and editing.

Karina Furtado Rodrigues: Conceptualization; Formal analysis; funding acquisition; Investigation; Methodology; Project administration; Resources; Supervision; Validation; Visualization; Writing – original draft; Writing – proofreading, and editing.

Breno Pauli Medeiros: Conceptualization; Data curation;Investigation; Visualization; Writing – original draft; Writing – proofreading, and editing.