http://dx.doi.org/10.21544/2359-3075.29210

# EXAMINING THE PERSPECTIVE OF PUBLIC POLICIES IN CYBER DEFENSE AREA: THE BRAZILIAN CASE

Tadeu Maciel[1]
Juliana Zaniboni[2]

## ABSTRACT

This article analyzes the importance of public policies aiming at cyberspace in Brazil in the period from 2000 to 2023. The question that guides the text is: how did the Brazilian governments in this period present their cyber defense objectives in their respective "National Defense White Papers", the 2008 and 2020 National Defense Strategy and other high-level national defense documents, transforming them into effective actions? The methodology adopted is exploratory research with a qualitative approach. The hypothesis of this research is that although there has been the creation of norms and the development of initiatives that demonstrate the greater importance of cyber defense for Brazil in the 21st century, we can verify the lack of initiatives marked by the conception of long-term public policies. This article is structured in three topics. The first one brings a succinct debate on public policies in the defense area. The second topic analyzes the development of norms and public policies in Brazil aimed at cyber defense. The third topic presents some policies adopted and examples of the cybernetic capacity obtained by this country.

**Keywords:** Brazil; Cyber Defense; Public Policies; Cybernetic Capacity.

[1] Universidade Federal Fluminense, Niterói, Rio de Janeiro — RJ, Brasil. E-mail: tadeummaciel@gmail.com — ORCID https://orcid.org/0000-0003-2591-4557.

[2] Universidade Federal Fluminense, Niterói, Rio de Janeiro — RJ, Brasil. E-mail: julianazaniboni@id.uff.br — ORCID https://orcid.org/0000-0001-9695-6661.

## INTRODUCTION

The advancement of information and communication technologies in the contemporary world affects different spheres and the defense of States is not separated from this dynamic. The evolution of computing technology, satellites, and the internet provided the formation of new spaces and forms of interaction between individuals, international organizations, companies, and governments. However, despite bringing many benefits and opportunities, the "cyberspace" environment also presented new vulnerabilities for all its users. Depending on how technological advances are used, it is possible to observe significant geopolitical changes in the international order, especially in guaranteeing the security of States and their populations (CEPIK, 2002; VILLA; BRAGA, 2018; NYE JR. 2020; PINTO; MEDEIROS, 2022).

There are some debates about the definition of cyberspace. In the National Defense White Paper of 2020, despite not limiting the concept, it is evident the importance of this "new" space to Brazilian National Sovereignty, which has been recognized as an operational domain, such as the land, sea, air, and outer space. In 2014, the Ministry of Defense launched the Military Cyber Defense Doctrine, which defines cyberspace as a virtual space, composed of computational devices connected through networks or not, where digital information transits are processed and/or stored (BRASIL, 2014, p. 18).

Although the informational layer, cyberspace isn't purely virtual. A distinction necessarily made is the separation between the Internet and cyberspace, which aren't synonyms: the first is an operational electronic/electromagnetic domain, and the second is central to the network of operational domains based on computers (LOBATO; KENKEL, 2015, p. 25). It means that cyberspace exists beyond the Internet, but the opposite isn't possible. Thus, the Internet represents a part, but not a whole, of this space.

Libicki (2009) divides cyberspace into three layers: physical, syntactic, and semantic. The physical layer corresponds to all necessary equipment to make cyberspace functional, like cables and wires. The syntactic layer refers to systems and protocols of machines, and the semantic contains the primary information and codes, which means the reason why computers exist. By understanding the complexity of cyberspace, as well as its dimensions, running through the physical and virtual scope, it becomes more comprehensive the need for protection of this space. Starting from spaces each time more automated, the vulnerabilities in cyberspace can be exploited, becoming a threat to the State and its infrastructures, which need to be carefully analyzed to give rise to public policies to face the dangers materialized in invasions, data theft, and the most diverse cyberattacks.

There are also debates about what exactly consists of the terms of cyberattack and cyberthreat. But, based on the vision of the Ministry of Defense in Brazil, cyberattack means actions to interrupt, deny, degrade, corrupt, or destroy computational information or systems stored in repository or computational networks and communications of opponents (BRASIL, 2014, p. 23). Besides, cyber threat means a potential cause of an unwanted incident that can result in damage to a cyberspace of interest (BRAZIL, 2014, p. 18).

Some examples of cyberattacks involving the Brazilian State can be cited. In political scope, in 2014 occurred a cyberattack when the hacking group Anonymous Brazil published stolen usernames and passwords on Brazilian government websites in the context of protests about the 2014 FIFA World Cup (KSHETRI, 2020, p. 86). In economic scope, involving cyberattacks in the financial sector, from 2012 to 2014 cybercriminals manipulated payments through bank payment slips, changing its information, and sending the money to the invader instead of the intended beneficiary (KESSEM, 2016). During this period, this action compromised approximately US$ 3.75 billion (TUBIN, 2014). Companies and users aren't the exclusive victims of cybercriminals. An example occurred in November 2020, when Superior Justice Tribunal was the target of a cyberattack, with ransomware kind, which means they encrypt the data, preventing access to the user, while hackers wait the rescue to be paid (ORTIZ, 2020).

In addition, still using Brazil as an example, according to the report "Digital Trends in the Americas Region 2021", carried out by the International Telecommunications Union, in 2019 the percentage of individuals who used the internet was 70% of the Brazilian population (ITU, 2021, p. 14). Regarding the proportion of households with internet access, from 2017 to 2019, Brazil presented 67% (ITU, 2021, p. 15). The greater presence of citizens on the internet, to perform various activities, requires more effective actions on the part of State entities to guarantee the security of this network and its users.

Based on this scenario, this article analyzes the implementation of cyber defense public policies in Brazil. The central question that guides the text is: how did the governments of Brazil in this period present their cyber defense objectives in their respective "National Defense White Papers", the 2008 and 2020 National Defense Strategy and other high-level national defense documents, transforming them into effective actions? The objective is to observe whether the propositions contained in these official documents provide government interventions that result in public policies, programs, projects, plans and effective actions in the field of cyber defense, within the adopted time frame. The hypothesis of this research is that although there has been the creation of norms and the development of initiatives that demonstrate the greater importance of cyber defense for Brazil in the 21st century, we can verify the lack of initiatives marked by the conception of long-term public policies.

This panoramic view of the public policies adopted by this country, in the period from 2000 to 2023, can contribute to verifying the capacity of cyber defense in Brazil. Capacity building is understood as the power to deter aggression and protect ICTs (Information and Communications Technologies) against threats, with a focus on government institutions. Specifically, we highlight in this article some actions of Brazilian governments for effective cybernetic capabilities in defense, as well as in the construction of physical infrastructures, the creation of cyber defense centers for this purpose, the acquisition of equipment, etc. This research effort is justified because the security and defense fields of this country have increased the investment in the development and updating of strategies and public policies focused on cybernetic issues, to promote the maintenance of sovereignty in cyberspace.

The methodology of this article is exploratory research, with a qualitative approach. A documentary analysis of official documents and bibliographic references on the subject is carried out, such as the National Defense Strategy of 2008 and 2020, the Green Book Cyber Security in Brazil of 2010, the White Paper on National Defense of 2012 and 2020, the National Strategy of Cybersecurity 2020 and the South American Defense Guide.

This article is structured in three topics, in addition to this introduction and final remarks. The first topic brings a succinct debate on public policies in the defense area. The second topic analyzes the development of norms and public policies in Brazil aimed at cyber defense. The third topic presents the public policies adopted and the cybernetic capacity obtained by this country.

## PUBLIC POLICIES IN THE DEFENSE AREA

The knowledge field of public policies has been consolidated as a multidisciplinary locus of well-known centrality. Studies in this area have been used to understand, among other elements, the limits and possibilities of State intervention around important socioeconomic issues. However, Rodrigues (2010) warns that there is no consensual concept of public policies. Besides the multiplicity of approaches that make up this field, Souza (2006) states that it is possible to summarize the concept of public policies as:

> the field of knowledge that seeks, at the same time, to "put the government into action" and/or analyze this action (independent variable) and, when necessary, propose changes in the direction or course of these actions (dependent variable). The formulation of public policies constitutes the stage in which democratic governments translate their electoral purposes and platforms into programs and actions that will produce results or changes in the real world. (SOUZA, 2006, p. 26).

In general, public policies involve a wide range of actors, demands, and interests, which are decisive for their formulation, implementation, monitoring, and evaluation process. As highlighted by Lotta (2019, p. 11), public policies can be analyzed as a "cycle that goes through different phases: agenda, formulation, implementation, and evaluation. This cycle does not necessarily match reality, but it is a relevant analytical instrument for understanding the decision-making processes that are part of public policies".

During these phases, public policies do not appear as the mere imposition of formulas and calculations for each problem but are usually the result of intense interaction among political actors, with their respective powers of influence (RUA, 2009). This dynamic should not be different when it comes to public policies in the field of defense, more specifically concerning the cyber area.

Almeida (2010, p. 221-3) states that "national defense must be understood as a public good provided to society through public policies". Such policies must be understood as "public" because they originate and are supported by the public power and must not, at least in principle, be constituted in the name of private interests or demands of the "market". Therefore, national defense is configured as a public good that, according to the constitutional-legal structure, must be a responsibility of the State and must benefit all citizens equally.[3]

> Public policies are 'public' - not private or just collective. Their 'public' dimension is given not by the size of the social aggregate on which they affect, but by their 'imperative' character. This means that one of their central characteristics is the fact that they are decisions and actions covered by the sovereign authority of the public power. (RUA, 1998, p. 2).

Like other public policies, Defense policy needs to be understood through the prism of different fields of knowledge and different social realities, otherwise, it can be transformed into a tangle of government actions that are incomprehensible to citizens and unable to obtain the necessary political-administrative support. As affirmed by Souza (2006, p. 36), public policies allow us to distinguish between what the government intends to do and what it does. Consequently, to avoid an excessive distance between discourse and practice, these policies must involve several actors and decision levels, reflecting the relationship between society and the State (PINHEIRO, 2014). Even if they are materialized by government agents, these policies are not necessarily restricted to formal participants, since the informal ones are also important.

In this sense, national defense must constitute a state policy and not a government policy. There must be a political arrangement underlying the national defense structure, which, by bringing together military and civilians, political parties, and society, allows it to be conducted above simple rivalries. The participation of various social sectors in the field of public defense policies is essential for building the legitimacy of the policies adopted. Defense policies in a democracy gain legitimacy as they involve the approval of the most diverse social actors, without losing the perspective of State responsibility in this process. This broad scope

[3] As highlighted by Almeida (2010), the provision of public defense policies does not conform to the notions of profit and price typical of the private sector, although this does not mean that the private sector or other sectors cannot participate in important activities to the provision of defense, as is the case of arms industry or research institutes.

for dialogue and active participation would be essential for efficient prioritization, resource allocation, consistency in implementation, and success in the ongoing monitoring process (ALMEIDA, 2010).

Many elements that characterize defense policies are the result of perceptions, in permanent mutation, of civilian politicians, the military, and civil society. Defense policy must have its purposes suited to national priority needs and, for that, the insertion of defense policy in the broader social debate is a step of first importance. Currently, given this scenario in Brazil, there has been great attention given to the guidelines about cyberspace, which has influenced the expansion of the state and society's demand for public policies in the field of cyber defense.

In general, according to Freitas and Pinto (2019, p. 32), the cyber defense would connect the power resources of the State and the direct threat to the sovereignty of this actor, so that the main object of defense is the public sector and their critical infrastructure. In line with this perspective, in the next topic, some understanding about how the concept of cyber defense is mobilized in Brazil will be presented.

## THE NORMATIVE ASPECTS OF CYBER DEFENSE IN BRAZIL

An important milestone for the issue of defense in Brazil in contemporary times was the creation of the National Defense Policy (PND) and the National Defense Strategy (END), bringing together instruments and forms of action aimed at National Defense. These documents would establish "the objectives and guidelines for the preparation and use of the Armed Forces in their mission of defending the homeland and guaranteeing constitutional powers" (BRASIL, 2012a, p. 7). In addition to the PND and the END, there is also the White Paper on National Defense, created in 2012 to present the context of national defense, as well as to expose in a more transparent way the numbers referring to the Ministry of Defense portfolio and its actions (BRASIL, 2012b). In this topic of the article, we analyze how the issue of cyber defense is presented in these documents.

In Brazil, the National Defense Strategy (END) establishes guidelines for the adequate preparation and training of the State (especially the Armed Forces) to guarantee the security and defense of the country both in peacetime and in crises. The first version of this document was released in 2008, which indicated that among the guiding principles of the defense development project for Brazil's capacity building would be three strategic sectors: space, nuclear, and cybernetics. For the government, the joint development of the space and cybernetic sectors would allow the country to develop autonomy in the matter, seeking not to depend on foreign technology (BRASIL, 2008). In this document, the government also made explicit the objective of collaborating with other countries for technological training. Subsequently, the END was revised and updated in 2012, 2016, and 2020.

The version of the END available in 2012 brought updates, defining priorities to ensure that the cyber sector would benefit from training in the industrial, educational, and military spheres. The priority was to strengthen the Cyber Defense Center (CDCiber) so that it could evolve into the Armed Forces Cyber Defense Command. Another relevant priority would be to encourage the training of their responsible institutions, such as the Ministry of Education and the Ministry of Defense, which should prepare a study for the creation of the National Cyber Defense School (ENaDCiber) (BRASIL, 2012a, p. 95). Therefore, the END seeks to establish mechanisms of action and strategies that expand the technological capabilities of the Armed Forces to guarantee cyber defense. In this sense, Oliveira et. al. (2017) emphasize that the END highlights the issue of sovereignty in the production of national technology for the best performance of the Armed Forces in guaranteeing cyber defense.

Also in 2012, the Brazilian National Defense White Paper was launched. According to this document, directive 14/2009 of the Ministry of Defense determined that the coordination of the cybernetic sector should be the responsibility of the Brazilian Army (BRASIL, 2012b). Therefore, the White Paper establishes premises for the cyber sector project, such as fostering the defense industrial base and inducing national industry to produce innovative systems.

The same document mentions that the Army's CDCiber, created in 2010, would be dedicated to improving the training of human resources; doctrinal updates; security strengthening; network incident responses; incorporation of lessons learned, and protection against cyber-attacks (BRASIL, 2012b). To this end, short-term actions were taken to consolidate the sector. Among them was the construction of the definitive headquarters of CDCiber and the implementation of projects in the sector, to expand the capacity to respond to cyber threats (BRASIL, 2012b).

It is interesting to note that the 2012 White Paper provides a forecast of expenditures on key strategic projects developed by the Army. Among them is the Cyber Defense project, which would have a total disbursement value estimated at R$ 895.40 million by 2023 (BRASIL, 2012b, p. 202). In 2012, the Cyber Defense Policy was also approved, to develop and keep up to date the Cybernetic Sector employment doctrine. Through this new policy, the Ministry of Defense sought to define the country's interests more effectively in cyberspace.

Two years later, in 2014, the Military Cyber Defense Doctrine (DMDC) was approved, which brought relevant guidelines for the sector. This doctrine divides actions in cyberspace into tactical, operational, strategic, and political decision-making levels. The first level is inserted into the subsequent one, alluding to the logic of an "onion", presenting itself in layers. This document places cyber defense at the strategic level, under the responsibility of the Ministry of Defense and the Armed Forces commands, while cyber security is planned at the highest governmental level by the Department of Information and Communications Security (DSIC), of the Institutional Security Office (GSI) of the Presidency of the Republic (BRASIL, 2014, p. 17)[4].

In that document, the cyber defense adopted by Brazil is defined as:

> the set of offensive, defensive and exploratory actions, carried out in Cyberspace, in the context of national planning at a strategic level, coordinated and integrated by the Ministry of Defense, with the purpose of protecting information systems of interest to the National Defense, obtain data for the production of Intelligence knowledge and compromise the opponent's information systems. (BRAZIL, 2014, p. 18).

The same document addresses the issue of cyber warfare, which would essentially cover actions in cyberspace to interfere with the adversary's capabilities. Based on this context, in its third chapter, the DMDC addresses what the Military Cyber Defense System (SMDC) is and how it works, since its creation in 2012. In general terms, the SMDC is:

[4] Regarding the difference between the terms "cyber security" and "defense", cybersecurity applies to the part of information security with a focus on digital protection, taking care of threats to information transported by cybernetic means. However, the growth of practices such as cyberterrorism and virtual crimes, which are increasingly present in our society, require the existence of exclusive cyber defense mechanisms, aiming at the creation of public policies that promote protection against threats or aggressions arising from digital media that may affect national security.

> a set of facilities, equipment, doctrine, procedures, technologies, services and personnel essential to carry out defense activities in Cyberspace, jointly ensuring their effective use by the FA, as well as preventing or hindering their use against the interests of the National defense. (BRASIL, 2014, p. 25).

The main initiative of the SMDC is the CDCiber, responsible for the actions of coordination and integration of the Cybernetic Sector, which would allow the Armed Forces to protect critical infrastructures (such as hydroelectric plants, financial systems, water supply, and electricity) against cyberattacks. In November 2020, the Military Cyber Defense System was activated and has ComDCiber as a central body (BRASIL, 2020).[5] The Center promotes integration between several institutions involved in Cyber Defense activities, such as the Center for Studies, Response and Treatment of Security Incidents in Brazil (CERT.br), Ministries, among others, as stated by Santos (2019, p. 14-15):

> CDCiber acted as a unified point of contact between government agencies and private companies regarding cyber defense. […] Including the various coordination meetings with representatives of the Brazilian Navy, Brazilian Army, Brazilian Air Force, Institutional Security Office of the Presidency of the Republic (CTIR.gov and ABIN), Serpro, DPF, Anatel, ANEEL, FURNAS, Angra dos Reis Nuclear Power Plant, ANAC, among other agencies, contributed to the establishment of mutual trust between the various agencies. (SANTOS, 2019, p. 14-15).

Although this integration effort with several essential entities (military and civilian) still needs to be expanded (NOBERTO, 2022), the Military Cyber Defense System seeks to promote the participation of non-military sectors of society, such as the academic community, civil society, and other parts of the public and private sectors, in addition to the defense industrial base, also endorsing international cooperation and interaction.

[5] The National Defense White Paper, in the updated version of 2020, brings some news about the sector, such as the creation of the Cyber Defense Command (ComDCiber), activated in 2016. From then on, ComDCiber was responsible for the main activities, as well as capacity building in the Cyber Defense Sector. In this way, entities such as CDCiber and ENaDCiber were subordinated to ComDCiber.

An example of this attempt is the Exercise of Cybernetics Guardian (ECG), which considered the major in cyber defense in the South Hemisphere. The main objective is to create and present a realistic space in which the participants' critical infrastructures need to be protected from cyber-attacks on their systems of Technology of Information and Operation. In ECG 4, which occurred in 2022, besides the Army, it was gathered more than 120 public and private organizations (CISO, 2020).

Brazil actively participates in international forums and cooperates with other countries to enhance its cyber defense capabilities. Another example of this would be the Budapest Convention on Cybercrime, signed by President Luiz Inácio Lula da Silva on 12 April 2023, adopting, for internal and external affairs, the Council of Europe Convention on Cybercrime. "The compact aims to promote international cooperation in the exchange of information on cybercrime and infractions requiring digital evidence stored in other countries" (NASCIMENTO, 2023).

These dynamics can be understood due to the characteristics of cyberspace, which bring implications and specificities that would escape the unique action of military agencies, which need the help of these other social sectors, either to build ways of guaranteeing and reinforcing cyber security and defense, or even in situations of threats, thus spreading the concentration of possibilities and forms of defense (VIANNA; CAMELO, 2020).

Finally, in its fourth chapter, the DMDC analyzes defense and cyber warfare in the operational field, presenting explanations, in general terms, on how operations of different types would be planned and carried out and what would be the categories of officers responsible for each area of responsibility. Therefore, from the implementation of the main elements mentioned above, the DMDC considered it possible to achieve its objective of "establishing the foundations of the Military Doctrine of Cyber Defense, providing unity of thought on the subject, within the scope of the Ministry of Defense (MD), and contributing to the joint action of the Armed Forces (AF) in the defense of Brazil in cyberspace" (BRASIL, 2014, p. 13).

The above reflection allowed us to point out some understandings, norms, and policies adopted by Brazil concerning cyber defense. In the next topic, some public policies adopted and the cybernetic capacity obtained by the country are listed. Information such as instruments acquired, training of human resources, seminars, forums, and cooperation on the subject are presented.

## BRAZILIAN CYBER DEFENSE CAPABILITY

As discussed in the topic above, the Brazilian cyber defense agenda has gained greater evidence since 2008, with the publication of END. According to Oppermann (2019, p. 6), one of the first major cyber challenges in Brazil occurred in June 2011, when a series of attacks took down Brazilian government websites, such as President Dilma Rousseff profile, Petrobras, IBGE, among other relevant websites from Brazilian states. In reaction to this episode, a series of debates on the topic gained greater emphasis in the governmental and academic spheres (OPPERMANN, 2019, p. 8).

Oppermann (2019, p. 10) also highlights the role of CDCiber in the 2014 World Cup and the 2016 Olympic Games. In addition to these major events, in 2012 Brazil also hosted RIO+20, the United Nations Conference on Sustainable Development, which inaugurated the monitoring of major events by CDCiber. It is worth mentioning that the other military forces also played important roles in the national security strategy during these major events, such as the Navy's Cyber Incident Treatment and Response Center, and the Air Force's Computer Network Incident Treatment and Response Teams.

Brustolin (2019) mentions that in 2017 there was another major cyber-attack that affected the Brazilian government. According to the author, several companies and public institutions suffered attacks on their websites and had to turn off their computers and interrupt their services, among them: Petrobras; National Social Security Institute (INSS); Courts of Justice of several Brazilian states; Ministry of Foreign Affairs; and the Brazilian Institute of Geography and Statistics (IBGE).

Another issue of insecurity brought up by Brustolin (2019) was the case of external interference in Brazilian elections through the so-called "fake news", false news triggered on social networks, with the use of fake profiles. The Superior Electoral Court even interfered to reduce the circulation of false information and cyber-attacks during the election period. Although this issue is not specifically about the area of cyber defense, but of cybersecurity, this situation demonstrates the dimension of the importance that cyberspace has for the State and society.

To expand its capabilities in cyber defense, the Brazilian State promoted and participated in several initiatives in the field. The country joined Argentina in the Ibero-American Cyber Defense Forum, hosting the

Ibero-American Cyber Defense Exercise in 2017.[6] In addition, according to the case study carried out by the organization "Article 19", entitled "Development of Security Policies Cybersecurity and Cyberdefense in South America", the country was involved in several projects that aimed mainly at international cooperation in the matter. According to "Article 19", Brazil sought to establish links with organizations such as UNASUR, Mercosur, and the Organization of American States (OAS), in addition to establishing bilateral relations, as was the case with cooperation with Argentina.

Taking this bilateral cooperation as an example, in 2013 Argentina and Brazil started dialogues to deal with the cybernetic sector. In that year, the Ministers of Defense of Brazil, Celso Amorim, and Argentina, Agustín Rossi, met to analyze bilateral cooperation in cyber defense, after a series of accusations of spying by the US government on citizens of both countries, including President Dilma Rousseff. At that meeting, the ministers agreed on the need for a greater exchange of information between specialized officers of the armed forces of each country (EXAME, 2013).

In September of that year, the two countries elaborated the "Declaration of Buenos Aires", in which the ministers, agreeing on the need to create a working group related to the subject, planned the visit of Argentine officers to the Center for Cybernetic Defense of the Brazilian Army and in the Cyber Warfare Course for Officers, held in 2014, and for non-commissioned officers, held in 2015.

On a second occasion, in November 2013, the "Joint Declaration of Brasilia" was prepared, and the 1st Meeting of the Bilateral Working Subgroup on Cyber Defense Cooperation (SCDC) was held. The SCDC played an important role in the cooperation between Brazil and Argentina. "Article 19" cites a list of 17 actions in which the subgroup acted and divided them into four categories: 1. Training (offering vacancies in courses from one country to another); 2. Doctrine (establishment of fundamental ideas about cyber defense); 3. Scientific research (activities to discover new knowledge and/or participation in seminars); 4. Direct cooperation (exchange of information between institutions about common procedures) (ARTICLE 19, 2017, p. 32).

These four categories of action allowed the bilateral relationship to promote development in the cybernetic sector for both countries,

[6] The Ibero-American Cyber-Defense Exercise mainly emphasizes the cooperation of member countries in the field of cyber-defense, both on a technical basis, in relation to the dissemination of information about attacks, both in academic exchange, with the promotion of training and courses in the area (MOYANO, 2020).

enabling the training of human resources. Since then, bilateral cooperation in this field has been revisited. For example, in 2019 the defense ministers of the two countries reaffirmed their commitment to the bilateral relationship in several areas, including fostering exchanges between academic institutions and Military Training Centers to develop a binational posture in cyber defense (BRASIL, 2019).

Regarding Brazil's actions with regional organizations, in the Southern Common Market (Mercosur), the main initiative in the area was the repudiation of US espionage in the countries of the region. In addition, some commitments were undertaken, such as the constitution of a working group to coordinate efforts, together with the South American Defense Council and the South American Infrastructure and Planning Council, to implement actions to make telecommunications in member countries and reduce dependence on foreign technology, a debate that became even more latent after the trade war between the United States and China over 5g technology.

At Union of South American Nations (UNASUR), while this organization was effectively active, efforts in cyber defense were concentrated on the South American Defense Council, through which a working group was created with meetings that took place in Lima, Peru, in 2012 and 2013, and Buenos Aires, Argentina, in 2014. Within the limited experience of the Forum for the Progress of South America (PROSUL), the Defense Working Group envisaged improving cooperation and information exchange in cyber defense, through protocols of exchange of information (BASTOS, 2021).

Within the Organization of American States (OAS), cooperation efforts focused on cybersecurity. In this sense, Brazil has participated in courses, seminars, and exercises on several occasions, even hosting relevant events such as the 2015 Internet Governance Forum, in João Pessoa, which had the participation of the representative of the Security Program Cybernetics of the OAS. In addition, in November 2021 the Hemispheric Conference on Cyber Defense was held by the Inter-American Defense Board, with the participation of 28 countries, including Brazil and Argentina.

As an internal initiative, one of the biggest highlights for training in cyber defense in Brazil was the "International Cyber Defense Internship for Officers from Friendly Nations".[7] Developed by the Army's Electronic

[7] In addition to military personnel from the Brazilian Armed Forces, representatives from twenty-seven countries, including: Germany, Angola, Argentina, Bolivia, Canada, Chile, China, Colombia, Ecuador, have participated in the International Cyber Defense Internship

Warfare Instruction Center (CIGE), its first edition was held in 2016 and since then it has been held annually. Its activities address several areas of cybernetic knowledge, such as forensic techniques, cryptography, vulnerabilities in Linux, Windows, and Web environments, and the development of cybernetic attacks (CIGE, 2023).

To evaluate public policies in cyber defense, the Federal Senate published, in 2019, the "Public Policy Evaluation Report: The National Policy on Cyber Defense", carried out by Senator Esperidião Amin. According to this report, in 2014 the Ministry of Defense created the Program for Cybernetic Defense in National Defense (PDCDN), with the aim of:

> [...] increasing training activities, doctrine, science, technology and innovation, intelligence and operations, within the scope of National Defense, through coordination and systemic integration, aiming to jointly ensure the effective use of cybernetic space (preparation and operational use) by the Ministry of Defense and the Armed Forces and prevent or hinder its use against the interests of National Defense. (SENADO FEDERAL, 2019, p. 12).

The report also mentions the budget allocated to the cyber defense area. In 2020, R$ 22 million was allocated to the Ministry of Defense and the Army for investment in the cybernetic sector. Of this amount, only R$ 6 million would be allocated to the Cyber Defense Command – ComDCiber. However, this institution stated that the amount of BRL 60 million would be needed to implement and modernize a model capable of meeting the needs of this strategic sector (SENADO FEDERAL, 2019, p. 56).

From the information above, Brazil seems to be making efforts to develop its capabilities in cyber defense. Participation in international organizations and the provision of training internships demonstrate that the country seeks to be, at the very least, a reference at the regional level about this issue, establishing cooperation with neighboring countries, as is the case of Argentina. In this example, Brazil is a great ally of the country and its policies for the cybernetic sector have been adopted as

for Friendly Nations Officers. , Spain, United States of America, Ghana, Guyana, Indonesia, Israel, Nigeria, Pakistan, Paraguay, Peru, Portugal, United Kingdom, Dominican Republic, Senegal, Sri Lanka, Suriname, Uruguay and Venezuela (CIGE, 2023).

a parameter in Argentine policy formulations. This could be observed in the lecture "Public Policies for Cyber Defense in Comparative Perspective - Argentine Republic", in which Argentine Major Mariano Gómez affirmed that the evolution of cyber defense in Argentina has the Brazilian Army as its main guide (GÓMEZ, 2019, p. 27).

However, we must also consider the lack of investment in the area, mainly due to the country's vulnerability to cyber-attacks. There is an urgent need to increase the sector's budget, allowing for an adequate development of long-term public policies, that make it possible to apply in a more structured way the knowledge acquired in meetings, events and cooperation projects established on the subject. For this, there is a need for greater debate with society, as a way of contributing to this policy effectively assuming its public character, based on a great debate with the various sectors involved in this issue. This would even help Brazil to establish a federal regulatory framework that guides the national cyber defense policy.

Although attempts to improve cyber defense, Brazil still faces some significant challenges, even though the country has enhanced cybersecurity capabilities. The first challenge is the rapidly evolving of cyber threats. As some examples showed previously, cybercriminals are becoming more sophisticated each day, employing advanced techniques to exploit vulnerabilities in cyberspace. A report data made by FortiGuard Labs indicates that Brazil was the second country more targeted in Latin America in 2022, with 103.16 billion attempts of cyber-attacks (FEBRABAN, 2023). In this sense, Brazil needs to foster cybersecurity research and development, and continuously update its defense strategies.

To go up against cyber criminals, it is necessary that skilled cybersecurity professionals are able to build a robust cyber defense workforce to attract and train experts in the field. Brazil should focus on implementing strong educational programs, and specialized training. More creating opportunities for collaboration between academia, industry, and government agencies to bridge the skills gap, besides the successful initiative of Exercise of Cybernetics Guardian.

Raising awareness and promoting a culture of cybersecurity among citizens and businesses can be another strategy to strengthen cyberspace. Brazil should invest in public awareness campaigns, capacity-building, and educational initiatives to educate individuals, companies, and organizations about the risks associated with cyber threats. This way, every individual should have a role in the defense of cyberspace.

Furthermore, the protection of critical infrastructure remains a priority concern. Some actions can be made in this sense, for example, the development of cybersecurity frameworks and standards to safeguard essential systems and services. And regular assessments and audits of critical infrastructure should be conducted to identify vulnerabilities and implement necessary security measures (PASQUALETTI, DÖRFLER; BULLO, 2015)

Therefore, we can state that there has been a significant increase in debates and government initiatives focused on cyber defense and cybersecurity issues in Brazil, but there is a pending matter of further advances, as is the case of investments in research and training in human resources. Besides that, studies on cyber defense need to be expanded and increasingly considered in public policies established for this area.

## FINAL CONSIDERATIONS

In contemporary times, the virtual environment is present in a large part of everyday life in society. As a result, cyber defense has become an important topic in International Relations and Strategic Studies on Security and Defense. Governments are constantly on the lookout for potential threats to national security, which leads them to produce tests for cyber threats, promote interdepartmental and interorganizational cooperation, and share information and best practices with friendly nations, for example.

In Brazil, an aspect that has been highlighted is the submission of the military apparatus to civilian control. This implies opening up greater possibilities for dialogue between civilians and the military in sensitive areas, such as the field of cyber defense. Even though this theme is a delicate topic, with implications that involve safeguarding sovereignty and national security, there is a need to seek forms of cooperation and exchange on the subject, in addition to creating spaces for the participation of sectors of society in public policies in the field of cyber defense. Although there has been the creation of norms and the development of initiatives that demonstrate the greater importance of cyber defense for Brazil in the 21st century, we can verify the lack of initiatives marked by the conception of long-term public policies.

This research was based on the importance that the theme has nowadays and on its unequivocal impact on the daily life of society since training in cyber defense affects not only the state apparatus itself but all individuals who use online services. Considering that a safe country must also guarantee its protection in the digital environment, the concern with the defense of cyberspace becomes an important object of broad social interest.

Finally, this article produced an introductory look at the topic, with space for expanding the research in several ways, such as the establishment of comparative analyzes between the policies adopted by Brazil, Argentina, and other countries in the cyber field. The expansion of these debates can contribute to the literature on the subject and help to reinforce the flow of knowledge on cyber defense.

# EXAMINANDO A PERSPECTIVA DAS POLÍTICAS PÚBLICAS NA ÁREA DE DEFESA CIBERNÉTICA: O CASO BRASILEIRO

## RESUMO

Este artigo analisa a importância de políticas públicas voltadas para a ciberdefesa no Brasil no período de 2000 a 2023. A pergunta que norteia o texto é: como os governos do Brasil nesse período apresentaram seus objetivos de ciberdefesa em seus respectivos "Livros Brancos de Defesa Nacional", a Estratégia Nacional de Defesa de 2008 e 2020 e outros documentos de alto nível da defesa nacional, transformando-os em ações efetivas? A metodologia adotada é a pesquisa exploratória, com abordagem qualitativa. A hipótese desta pesquisa é que embora tenha havido a criação de normas e o desenvolvimento de iniciativas que demonstrem a maior importância da defesa cibernética para o Brasil no século XXI, podemos verificar a falta de iniciativas marcadas pela concepção de políticas públicas de longo prazo. Este artigo está estruturado em três tópicos. O primeiro traz um debate sucinto sobre as políticas públicas na área de defesa. O segundo tópico analisa o desenvolvimento de normas e políticas públicas no Brasil voltadas para a defesa cibernética. O terceiro tópico apresenta algumas políticas adotadas e exemplos da capacidade cibernética obtida por este país.

**Palavras-chave:** Brasil; Defesa Cibernética; Políticas Públicas; Capacidade Cibernética.

## REFERENCES

ALMEIDA, Carlos W. Política de defesa no Brasil: considerações do ponto de vista das políticas públicas. **Opinião Pública,** Campinas, v. 16, n. 1, p. 220-250, jun. 2010.

ARTICLE 19. **Desenvolvimento de políticas de cibersegurança e ciberdefesa na América do Sul** - Estudo de caso sobre a atuação governamental brasileira. São Paulo, Artigo 19, Brasil, 2017.

BASTOS, Eduardo H. S. **O Brasil e o diálogo de defesa Sul-americano no foro para o progresso e integração da América do Sul (PROSUL).** Dissertação em Ciências Militares, Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.

BRASIL. **Estratégia nacional de defesa.** Brasília, DF, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm. Acesso em: 17 ago. 2021.

BRASIL. **Política nacional de defesa e estratégia nacional de defesa.** Brasília, DF, 2012a. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf. Acesso em: 17 ago. 2021.

BRASIL. **Livro branco de defesa nacional.** Brasília, DF, 2012b. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/2012/mes07/lbdn.pdf. Acesso em: 25 jan. 2022.

BRASIL. **Doutrina militar de defesa cibernética.** Ministério da Defesa, Brasília, DF, 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 19 set. 2022.

BRASIL. **Planejamento estratégico setorial 2020-2031.** Brasília, DF, 2019. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/lai/institucional/diagra_planejamentoa_estrategicoa_17a_04a_2020.pdf. Acesso em: 17 ago. 2021.

BRASIL. Ministério da Defesa. **Decreto nº 9637, de 16 de novembro de 2020.** Diário Oficial da União: seção 1, Brasília, DF, 17 nov. 2020. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 22 jan. 2022.

BRUSTOLIN, Vitelio. Comparative analysis of regulations for cybersecurity and cyber defence in the United States and Brazil. **Revista Brasileira de Estudos de Defesa.** v. 6, n. 2, p. 93-123, jul./dez. 2019.

CIGE. **Estágio internacional de defesa cibernética.** Comando de Comunicações e Guerra Eletrônica do Exército. Brasília, 2023. Disponível em: http://www.cige.eb.mil.br/index.php/en/estagio-internacional-de-defesa-cibernetica.  Acesso em: 20 mar. 2023.

CISO ADVISOR (2022). **Começa o exercício guardião cibernético 4.0.** Disponível em: https://www.cisoadvisor.com.br/comeca-o-exercicio-guardiao-cibernetico-4-0/. Acesso em: 22 de maio de 2023.

CEPIK, Marco. Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação. **Security and defense studies review**, v. 2, p. 246-267, Winter, 2002.

EXAME. Brasil e Argentina avançam na cooperação em ciberdefesa. **Revista Exame**, São Paulo, 22 nov. 2013. Disponível em: https://exame.com/tecnologia/brasil-e-argentina-avancam-na-cooperacao-em-ciberdefesa/. Acesso em: 11 jul. 2022.

FEBRABAN. Brasil é segundo país mais atingido por ciberataques na América Latina, diz relatório. **Febraban Tech**, 21 mar. 2023. Disponível em https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio. Acesso em: 22 maio 2023.

FREITAS, Riva S. ; PINTO, Danielle J.A. **Segurança e defesa cibernética: uma perspectiva das iniciativas legislativas na América do Sul**. *In*: XXVIII Encontro Nacional do CONPEDI, 2019, Goiânia.

FOLSOM, Thomas. Defining cyberspace - Finding real virtue in the place of virtual reality. **Tulane journal of technology & intellectual property**, vol. 9, p. 75-121, 2007.

GÓMEZ, Mariano O. **Políticas públicas de defesa cibernética em perspectiva comparada – República Argentina**. *In*: Ciclo de Estudos Estratégicos. Rio de Janeiro, 2019. Disponível em: http://www.eceme.eb.mil.br/images/docs/PalestrasCEE/POLITICAS_PUBLICAS_DE_DEFESA_CIBERNETICA.pdf. Acesso em: 25 jan. 2022.

ITU, International Communication Union. Digital trends in the Americas region 2021: information and communication technology trends and developments in the Americas region, 2017-2020. **ITU Publications**, Americas, 2021.

KESSEM, Limor. The Brazilian malware landscape: a dime a dozen and going strong. **Security intelligence**, 21 jul. 2016. Disponível em: https://securityintelligence.com/the-brazilian-malware-landscape-a-dime-a-dozen-and-going-strong/. Acesso em: 20 maio 2023.

KSHETRI, Nir; DEFRANCO, Joanna F. The economics of cyberattacks on Brazil. computer, **IEEE Computer**, p. 85-90, 2020.

KUEHL, Daniel T. From cyberspace to cyberpower: defining the problem. **Cyberpower and national security**, Lincoln: University of Nebraska Press, v. 53, n. 9, p. 24-42, 2011.

LIBICKI, Martin. **Cyberdeterrence and cyberwar**. Pittsburgh: RAND Corporation, 2009.

LOBATO, Luísa C.; KENKEL, Kai M. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, v. 58, n. 2, p. 23-43, 2015.

LOTTA, Gabriela (org.). **Teorias e análises sobre implementação de políticas públicas no Brasil**. Brasília: Enap, 2019.

NASCIMENTO, Luiz. Agência Brasil. **Brazil ratifies Budapest Convention on cybercrime:** service providers may be required to disclose user data, 2023. Disponível em: https://agenciabrasil.ebc.com.br/en/geral/noticia/2023-04/brazil-enacts-convention-cybercrime. Acesso em: 22 maio 2023.

NOBERTO, Cristiane. Brasil salta para 18ª posição em ranking mundial de cibersegurança. **Correio Braziliense**, 20 jun. 2022. Disponível em: https://www.correiobraziliense.com.br/politica/2022/06/5016461-brasil-avanca-em-ranking.html. Acesso em: 10 ago. 2022.

NYE JR., Joseph. **Cyber power**. Harvard Kennedy School, Belfer Center for Science and International Affairs, maio 2020.

OLIVEIRA, Marcos G. *et al*. **Guia de defesa cibernética na América do Sul.** UFPE, 2017.

OPPERMANN, Daniel. A discourse analysis of cyber defense in Brazil. **Anais do 7° Encontro da Associação Brasileira de Relações Internacionais**, Belo Horizonte, MG, 2019.

ORTIZ, Brenda. Por suspeita de ataque hacker, TRF-1 retira do ar portal da Justiça Federal do DF e de 13 estados. **G1**, 27 nov. 2020. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2020/11/27/por-suspeita-de-ataque-hacker-trf-1-retira-do-ar-portal-da-justica-federal-do-df-e-de-13-estados.ghtml. Acesso em: 21 maio 2023.

PASQUALETTI, Fabio; DÖRFLER, Florian; BULLO, Francesco. Control-theoretic methods for cyberphysical security: geometric principles for optimal cross-layer resilient control systems. **IEEE Control Systems Magazine**, p. 110-127, 2015.

PINHEIRO, Luíza M. **O Centro de gestão e estudos estratégicos e as políticas públicas de estado**. Monografia (Bacharelado em Ciências Sociais). Universidade de Brasília. Brasília, DF, 2014.

PINTO, Danielle J.A.; MEDEIROS, Sabrina E. Inteligência artificial e seu uso no contexto militar: desafios e dilemas éticos. **Cadernos Adenauer XXIII**, n. 2, p. 97-113, 2022.

RODRIGUES, Marta M. A. Políticas públicas, coleção. **Folha Explica**, São Paulo: Publifolha, 2010.

RUA, Maria das Graças. **Análise de políticas públicas:** conceitos básicos. *In:* RUA, Maria das Graças; VALADAO, Maria Izabel. O Estudo da Política: temas selecionados. Brasília: Paralelo 15, 1998.

RUA, Maria das Graças. **Políticas públicas**. Florianópolis: Departamento de Ciências da Administração, UFSC; [Brasília]: CAPES: UAB, 2009.

SANTOS, Bruno Ígaro L. **O emprego da capacidade cibernética nas operações militares em grandes eventos no Brasil:** emprego do centro de defesa cibernética nos jogos olímpicos de 2016. Dissertação em Ciências Militares, Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2019.

SENADO FEDERAL. **Relatório de Avaliação de Política Pública**: a política nacional sobre a defesa cibernética. Senado Federal, Brasília, DF, 2019. Disponível em: http://legis.senado.leg.br/sdleg-getter/documento?dm=8054598&ts=1576151 065975&disposition=inline. Acesso em: 20 jan. 2023.

SOUZA, Celina. Políticas públicas: uma revisão da literatura. **Sociologias**, Porto Alegre, v. 8, n. 16, p. 20-45, jul/dez 2006.

TUBIN, George. Boleto malware targeting brazilian banks. **Security intelligence**, 10 jul. 2014. Disponível em: https://securityintelligence.com/boleto-malware-two-new-variants-discovered/. Acesso em: 21 maio 2023.

VIANNA, Eduardo W.; CAMELO, José R. S. Defesa cibernética no Brasil: primícias de uma história de sucesso. **Revista da Escola Superior de Guerra**, v. 35, n. 75, p. 127-154, set./dez. 2020.

VILLA, Rafael D.; BRAGA, Camila de M. Segurança internacional. *In*: SAINT-PIERRE, Héctor L.; VITELLI, Marina G.. (org.). **Dicionário de segurança e defesa.** São Paulo: Editora Unesp Digital, p. 1047-1056, 2018.

*** Recebido em 01 de janeiro de 2023, e aprovado para publicação em 18 de julho de 2023.**