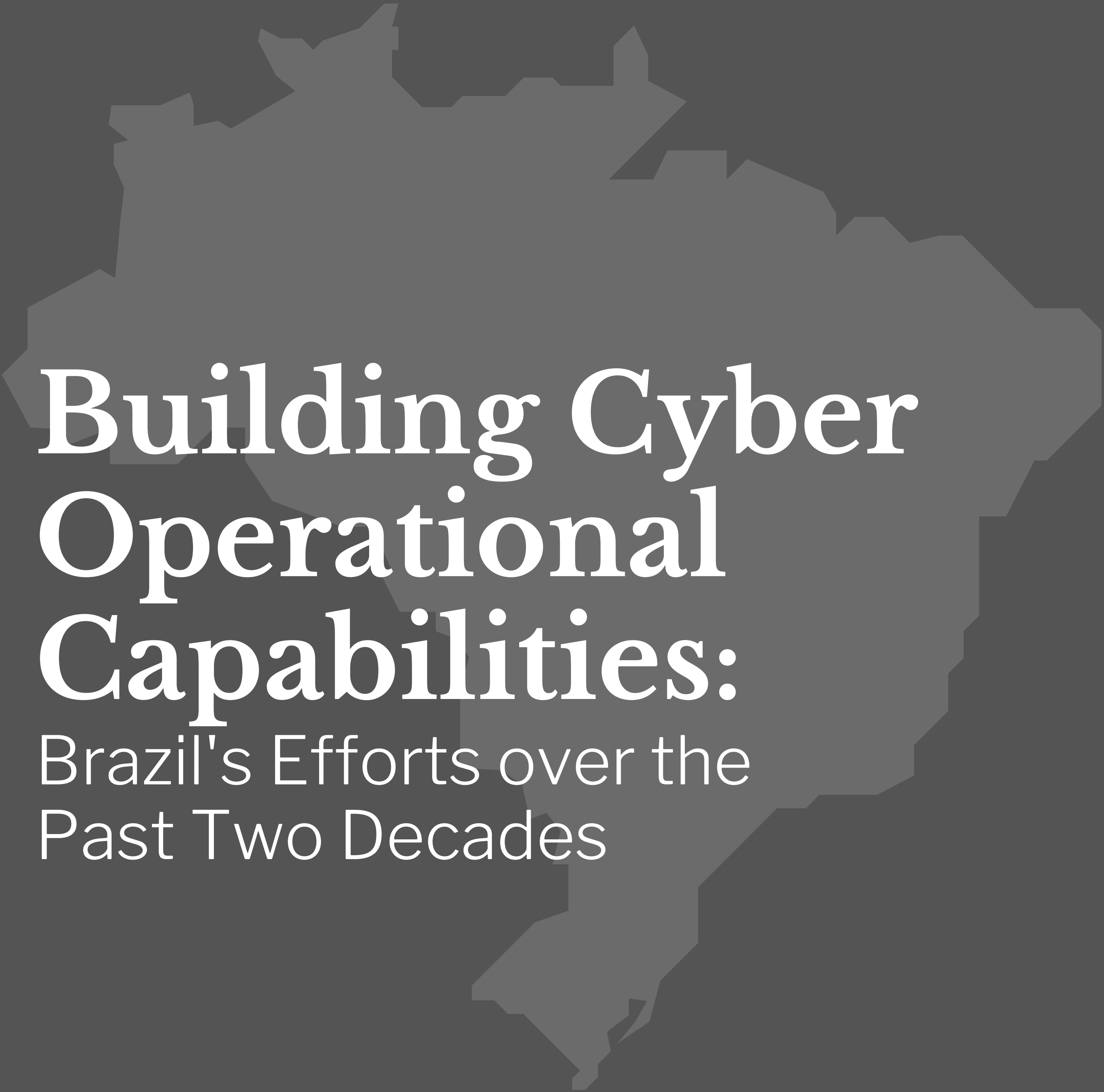
INTERNATIONAL CYBER OPERATIONS RESEARCH PAPER SERIES Paper 2



Building Cyber Operational Capabilities:

Brazil's Efforts over the Past Two Decades

Barbara Marchiori de Assis

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This study was produced by an external consultant, contracted to produce studies for the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of France, Germany, the Netherlands, Norway and Switzerland, and by Microsoft. Gratitude is extended to Giacomo Biggio, Renata Hessmann Dalaqua and Giacomo Persi Paoli for offering their thoughts on this paper. Design and layout of the publication: Eric M. Schulz.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

About the Author

BARBARA MARCHIORI DE ASSIS is a cybersecurity policy specialist with a Master's in Public Administration from Cornell University (2014).

TABLE OF CONTENTS

On the Research Paper Series

The number of States possessing the capability to conduct international cyber operations against or through foreign information and communications technology infrastructure is on the rise. These cyber operations can signal a mounting large-scale threat to the security of a State, could be understood as a violation of sovereignty and may lead to an escalation.

To facilitate transparency, advance trust among States and thus promote stability in international cyberspace, the UNIDIR Security and Technology Programme commissioned a series of research papers outlining national capabilities to conduct international cyber operations and relevant national doctrines regulating the conduct of such operations. In the resulting papers, nine scholars and practitioners provide an overview of the capabilities and doctrines pertaining to 15 countries across different regions: Australia, Brazil, Canada, China, France, Germany, India, the Islamic Republic of Iran, Israel, Japan, the Republic of Korea, the Russian Federation, Saudi Arabia, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

To read more about the research paper series, please refer to the "International Cyber Operations: National Doctrines and Capabilities" paper, available at www.unidir.org/cyberdoctrines.

Andraz Kastelic

Lead Cyber Stability Researcher,
Security and Technology Programme, UNIDIR

Introduction

This paper describes the evolution of cyber defence in Brazil, from early discussions in the 2000s to specific policies and measures implemented to develop the national capability to conduct international cyber operations if necessary. Although Brazil has been strengthening its cyber defence capacity for the past two decades, the major international events hosted by the country from 2012 to 2016, such as the World Cup and the Olympic Games,[1] marked a watershed in Brazil's cyber defence capacity development. During this period, not only did Brazil solidify its cyber defence military structure, it also developed a cyber defence doctrine aimed at unifying concepts and guiding operations in cyberspace.

According to the Brazilian Cyber Defence Military Doctrine, cyber defence consists of offensive, defensive and exploratory operations in cyberspace. This definition is of paramount importance since it has guided the development of cyber defence capacity towards enabling the country to conduct such operations in cyberspace if needed. However, in contrast to other strategic fields, such as nuclear and outer space, operations in cyberspace do not have the same level of international control mechanisms in place.[2] Brazil's defence strategic documents have underscored concerns over potential conflicts in cyberspace in the near future and the importance of developing the capacity to enable the country's response in a timely and appropriate manner.

Although Brazil has several cyber defence guidelines and directives, most of these documents are related to cyber defence at the operational and tactical levels, not the political level. Information about the country's cyber defence policies is extensively available online, albeit not necessarily in a well-structured manner or in a format easy for outsiders and strangers to the cyber defence sector to understand. This is mostly due to the lack of a unified cyber defence legal framework in the country. The lack of national cyber defence law might negatively impact how key cyber defence decisions – with potential international impact – are made in the country.

This paper is composed of four sections beyond this introduction. Section 2 describes the development of cyber defence capacity in Brazil in the past decades. Section 3 analyses the cyber defence framework, examining cyber defence concepts and how the national defence policies address the cyber defence issue and increased concern over cyber conflicts. Section 4 considers the relationship between cyber defence and cybersecurity in Brazil. The paper concludes, in Section 5, with the major challenges that could hinder the Brazilian cyber defence sector's consolidation and the way forward.

[1] Rio + 20 in 2012, World Youth Day 2013, the 2013 FIFA Confederations Cup, the 2014 World Cup, and the 2016 Olympic and Paralympic Games in Rio de Janeiro.
[2] Escola Superior de Guerra (2016, 13).

Building Cyber Defence Capacity (2000–2020)

In this paper, the cyber defence capacity development in Brazil is divided into three stages. The first, the formative stage, describes when cyberspace became a strategic sector and when Brazilian defence policies started to directly address this matter. The second stage, the development stage, is marked by the major events hosted by Brazil from 2012 to 2016. These events were key drivers that prompted investments in the sector and the creation of cyber defence units within the Brazilian Armed Forces. The third is the consolidation stage, during which projects that were planned in previous stages were finally implemented. The discussion of the consolidation stage also includes future challenges and trends.

FORMATIVE STAGE: CYBERSPACE AS A STRATEGIC DOMAIN (2000–2011)

The publication of the first National Defence Policy in 1996,[3] followed by the creation of the Ministry of Defence in 1999,[4] gave rise to Brazil's modern view on national defence. The vision is aligned with the country's overall development policy, which encourages greater engagement with different sectors, as described in several defence documents prepared throughout the past two decades.[5] However, it was only in the mid- and late-2000s that the national defence framework advanced, with the revision of the National Defence Policy in 2005[6] and the publication of the National Defence Strategy in 2008.[7] The 2005 National Defence Policy briefly mentioned the risk of cyberattacks but did not provide much information.

Cyberspace would only officially become a strategic sector for defence in 2008. Specifically, the 2008 National Defence Strategy recognized cyberspace as one of the strategic domains for national defence, alongside the nuclear sector and outer space.[8] Mostly, the 2008 National Defence Strategy highlighted the importance of building both human and technological cyber defence capacity within the Armed Forces to prevent Brazil from relying on other countries' technology; however, the strategy did not indicate how such goals would be achieved.

In 2009, instead of creating a "fourth force" devoted to cyber defence and cyber warfare, the Ministry of Defence assigned the responsibility for coordinating cyber defence initiatives to the Brazilian Army.[9] The Army's Science and Technology Department was in charge of formulating a project for the cyber sector, the Cyber Defence Strategic Project.[10] The implementation of a cyber sector within the Army started in July 2010,[11] and the Cyber Defence Strategic Project encompassed several foundational projects to be carried out from 2011 to 2014, such as the development of technological and research capacity as well as of a governance structure.[12]

In August 2010, the Army decided to create the Cyber Defence Center (CDCiber). As a first step, the Army established a "nucleus" of CDCiber to better coordinate and integrate cyber defence efforts.[13] The CDCiber nucleus functioned as a working group to prepare CDCiber for its actual launch. The nucleus was responsible for implementing the above-mentioned foundational projects. A similar methodology – that is, the establishment of a nucleus and, later, the unit's actual establishment – was applied in the development of subsequent cyber defence units in Brazil.[14]

The first mission of CDCiber would take place in July 2012 during the Rio + 20 event. From 2010 to 2012, CDCiber focused on building its cybersecurity capacity, which included developing the capacity to

[3] Brazil, Presidency (1996).
[4] Brazil (1999).
[5] Cordeiro (2016, 7).
[6] Brazil (2005).
[7] Brazil (2008).
[8] Brazil (2008).
[9] Brazil, Ministry of Defence (2009).
[10] Brazil, Army Commander (2009).
[11] Brazil, Army Commander (2010a).
[12] Costa (2013).
[13] Brazil, Army Commander (2010b).
[14] SegInfo (2014).

conduct military intelligence and prevent breaches of military critical information.[15] In 2012, CDCiber officially integrated the Army's organizational structure, and the Ministry of Defence assigned the centre the responsibility to coordinate and integrate cyber defence activities.[16]

The cyber defence framework continued to develop throughout the 2010s owing to the preparations for the major events from 2012 to 2016. Despite not being the target of any significant cyberattack, Brazil had the fourth highest cybercrime rate, by country, in 2011. The cybercrime cost in Brazil was estimated to be around USD 15 billion in that year.[17]

DEVELOPMENT STAGE: THE MAJOR EVENTS (2012–2016)

In 2012, the government reviewed the National Defence Policy and the National Defence Strategy and published the first version of the National Defence White Paper.[18] Since then, the executive branch, through the Ministry of Defence, has revised these documents every four years and submitted them to the Federal Congress for appraisal.[19] In 2012, the Ministry of Defence published the Cyber Defence Policy,[20] which aimed to guide cyber defence activities (at the strategic level) and cyber warfare (at the operational and tactical levels), as well as define the goals and directives for the Armed Forces. The Cyber Defence Policy's directives were also geared towards securing the major events taking place in the country from 2012 to 2016.

To reach the cyber defence sector's goals, the Cyber Defence Policy determined the conception and implementation of the Cyber Defence Military System, which was intended to comprise both military and civilian personnel and encompass CDCiber. The Ministry of Defence adopted a three-pronged approach entailing the government, academia and national industry. By creating the Cyber Defence Military System, the Ministry of Defence intended to set up the much needed institutional structure to better coordinate the country's cyber defence efforts. For instance, the Cyber Defence Military System would be responsible for identifying skilled individuals within the Armed Forces to compose the newly created system, organizing educational programmes to train professionals for the Brazilian cyber defence sector, conducting data analysis research, and formulating the Cyber Defence Military Doctrine.[21] Approved in 2014, the latter unified the

[15] Tanji (2012).
[16] Brazil (2012a); Brazil, Ministry of Defence (2012d).
[17] DefesaNet (2012).
[18] The goal of the National Defence White Paper was to provide more transparency about the Armed Forces' work to Brazilian society, while also informing Brazil's military motivations and building trust with the international community.
[19] Brazil (1999); Brazil (2010).
[20] Brazil, Ministry of Defence (2012c).
[21] Brazil, Ministry of Defence (2014c).

cyber defence concepts to coordinate and guide efforts among the Armed Forces.

In addition to the cyber defence policy framework, the major international events hosted by the country from 2012 to 2016, coupled with the leaks exposing the US spy programme in 2013, contributed to strengthening Brazil's cyber defence capacity. Major events are usually defined by their attractiveness to visitors, high investments, large media coverage and internationality, serving as important geopolitical and soft power tools for States.[22] Given the high-profile individuals, organizations and assets involved, events of this magnitude are a target-rich setting for cyberattackers. The Rio + 20 in 2012, World Youth Day 2013, the 2013 FIFA Confederations Cup, the 2014 World Cup, and the 2016 Olympic and Paralympic Games in Rio de Janeiro yielded significant investments in the country's cyber defence capability. Such investments included establishing specialized cyber defence units and contributed to enhancing cross-sectoral collaboration among militaries, government agencies and the private sector.

The Armed Forces can only be deployed in specific cases. For instance, the Joint Staff of the Armed Forces, which coordinates the Armed Forces' three branches (i.e. Army, Navy and Air Force), was responsible for securing the Rio + 20 event and deployed 15,000 military personnel to work on the event's security.[23] As mentioned, CDCiber's first mission was to coordinate cybersecurity efforts with the private sector and other government agencies during the Rio + 20.[24] Specifically, this mission consisted of monitoring the event's network, identifying potential vulnerabilities and protecting the communication system from potential cyberattacks. The Ministry of Defence was also authorized to temporarily deploy the Armed Forces to carry out cybersecurity and cyber defence activities in the Brazilian host cities of the 2014 World Cup and the 2016 Olympic Games.[25] During the World Cup, there were 756 cyber events, but no major incident occurred.[26]

The leaks exposing the US spy programme not only catalysed greater investment in cyber defence but also brought to the attention of Brazil's Federal Congress the importance for national security of protecting cyberspace. In September 2013, the Federal Congress established a parliamentary committee of inquiry to investigate not only the alleged US spy programme and its interest in Brazilian strategic and classified information but also the vulnerabilities of the Brazilian cyber defence and intelligence system.

After organizing several hearings with specialists from government agencies of the cyber and intelligence fields (e.g. Ministry of Defence, National Telecommunication Agency, federal police) and the purported targets of espionage (e.g. Petrobras), the parliamentary committee of inquiry concluded its work in April 2014.[27] Its report underscored the lack of an "intelligence culture" in the public and private sectors, since the topic was not widely discussed in Brazilian society. Plus, the report highlighted that intelligence activity was still perceived as an authoritarian remnant of the last Brazilian dictatorship (1964–1985). As a result of this lack of culture, the intelligence and defence sector did not have adequate funding or an adequate legal framework.[28] The report identified significant cuts in the cyber defence budget, especially when comparing the amount initially planned for each year with the amount allocated.

The scope of the National Defence Strategy and Cyber Defence Policy was limited to the military sector – as it should be. The report concluded that the formulation of a more comprehensive national cybersecurity strategy was required.[29]

Concerning cyber defence, the report recommended investing in research, development and innovation to build a cyber defence national industry, as well as conducting cyber defence simulation exercises with the participation of the private and public sectors.

Given the claims that the US National Security Agency spied on Brazilian oil and energy companies in June 2013, the Ministry of Defence also created a working group in September 2013 to identify cyber defence initiatives for immediate action.[30] In March 2014, in addition to suggesting measures to mitigate vulnerabilities in cyberspace, the working group's report recommended creating other cyber

[22] CSS (2019, 6–7).
[23] Brazil, Ministry of Defence (2012a, 178).
[24] Tanji (2012).
[25] Brazil, Ministry of Defence (2012b).
[26] Brazil, Federal Senate (2019, 18).
[27] Brazil, Federal Senate (2014).
[28] In December 2019, the federal Senate assessed the cyber defence public policy in Brazil and, once again, identified the lack of funding and adequate legal framework as the main constraints on the development of the sector.
[29] The National Cybersecurity Strategy was finally published in February 2020.
[30] Brazil, Ministry of Defence (2013).

defence units, such as the Cyber Defence Command (ComDCiber) and the National School of Cyber Defence. The 2012 National Defence White Paper had already stated the importance of developing a Cyber Defence Command[31] and indicated the need to prepare a study to create the National School of Cyber Defence.[32] The spying claims contributed to putting these plans in motion.

In 2014, the Ministry of Defence created the Cyber Defence Program in the National Defence, which is jointly coordinated by the Armed Forces, and sought to enhance the interoperability of cyber defence among the three branches.[33] In October 2014, in the framework of this programme, the Ministry of Defence issued directives for the creation of the ComDCiber and the National School of Cyber Defence.[34] The Joint Staff of the Armed Forces was responsible for supervising the implementation of the ComDCiber and the National School of Cyber Defence, both subordinated to the Army Command. These new cyber defence units would be composed of military personnel from the Armed Forces' three branches. Like the process for developing CDCiber, both institutions started with a nucleus dedicated to building the cyber capacity required for the establishment of the units.[35] During this time, the creation of the Cyber Defence Observatory was envisioned; the implementation of the observatory would start in June 2019.

CONSOLIDATION STAGE (2016–)

In more recent years, after these major events, the consolidation of the Cyber Defence Military System in Brazil has been noticeable.[36] The major events prompted the government to authorize the creation of the ComDCiber and the National School of Cyber Defence to compose the Cyber Defence Military System, together with CDCiber. The years from 2016 are marked by the establishment of these cyber defence units and long-term policies to allow their continuous improvement.

In 2017, the Army's Cyber Defence Strategic Project was elevated to a programme, becoming the Cyber Defence Strategic Program,[37] which encompasses several projects aimed at providing freedom of action for the Brazilian Army in cyberspace and enabling cyber operations against adversarial action.[38]

The ComDCiber started its operations on 15 April 2016. The ComDCiber is responsible for planning and supervising the cyber defence sector's operational, training and doctrinal activities. Both CDCiber (responsible for operational and intelligence activities) and the National School of Cyber Defence (responsible for promoting cyber defence education) are subordinated to the ComDCiber.[39]

The project for the establishment, consolidation and continuous improvement of the ComDCiber spans from 2016 to 2035 and is divided into three phases: (1) implementation and consolidation (2016–2022), (2) modernization (2023–2028), and (3) evolution (2029–2035).[40] This project is part of a comprehensive Cyber Defence Project coordinated within the framework of the Defence Articulation and Equipment Plan,[41] which is a long-term plan to enhance the Armed Forces' capacity to ensure foreign technological independence and strengthen the domestic defence industry. The plan focuses not only on equipment modernization but also on national defence governance and coordination.

In February 2019, the National School of Cyber Defence started its operations.[42] The school's mission is to foster cyber defence capabilities and contribute to the research, development and management of cyber defence. Its teaching structure is two-pronged: civil and military. Courses and internships are available to military personnel from the Armed Forces and friendly States, as well as the academic community. For instance, there have been discussions between the National School of Cyber Defence and the Ministry of Science, Technology, and Innovation to equip civil servants with the skills and knowledge to prevent and respond to cyber incidents.[43]

[31] Brazil, Ministry of Defence (2012a, 322).
[32] Brazil, Ministry of Defence (2012a, 354).
[33] Brazil, Federal Senate (2019).
[34] Brazil, Ministry of Defence (2014b).
[35] Brazil, Army (2015a); Brazil, Army (2015b).
[36] Brazil, Ministry of Defence (2020b).
[37] Brazil, Ministry of Defence (2019, 84).
[38] Brazil, Army (2021, 93).
[39] Brazil, Ministry of Defence (2020a, 47).
[40] Brazil, Army (2016).
[41] Brazil, Ministry of Defence (2020c).
[42] DefesaTV (2019).
[43] Brazil, Federal Senate (2019, 20).

In June 2019, the Cyber Defence Observatory was created as a partnership between the Army and the Federal University of Pernambuco in the framework of the Cyber Defence Program in the National Defence. Implemented by the ComDCiber and university faculty, the observatory will be a platform by which the academic, private and military sectors will collaborate and share information.[44]

Notwithstanding the continued implementation of cyber defence projects and units, the 2019 management report of the Army[45] reveals that the budget's downward trend may impact the continued improvement of the sector. Although the cyber defence structure in place could mitigate the impact of cyberattacks, the 2019 report stressed the importance of creating tactical structures to enable cyber offensive, defensive and exploratory operational capability.[46] Indeed, in December 2019, the Federal Senate issued a report[47] recommending continued and more robust investments in the sector, claiming that the current investments were insufficient.[48]

Similarly, the 2020 management report of the Army restated that budget constraints could put the continued implementation of the country's cyber defence and warfare structure at risk, delaying the execution of current projects.[49] The report also highlighted that the 2020 goal to fully implement the Cyber Defence Military System and the overall cyber defence and warfare structure was not achieved: only 70% was implemented, likely an indirect impact of the COVID-19 pandemic, and the Army expects to reach the original goal once normality resumes.[50]

All the cyber units, policies, programmes and projects mentioned in this section were created through presidential decrees or ordinances of the Ministry of Defence. Brazil's cyber defence policy is mostly based on administrative rules rather than on the legal framework defined by the legislative branch. Although the presidency and the Ministry of Defence are vested with the authority to issue such rules regarding cyber defence, a unified legal framework could assist not only the consolidation of the cyber defence sector but also the budget. Also, most of the current cyber defence governance and agenda is based on the lines of action defined during the preparations for the major events. In other words, there is a need to review the cyber defence agenda looking to the future.

[44] Brazil, Army (June 2019a).
[45] Brazil, Army (2019b).
[46] Brazil, Army (2019b, 22).
[47] Brazil, Federal Senate (2019).
[48] Brazil, Federal Senate (2019, 58).
[49] Brazil, Army (2021, 41).
[50] Brazil, Army (2021, 91).

Cyber Defence Framework

In addition to developing its cyber defence capacities in the past decades, Brazil has relevant policies, strategies and doctrines. The National Defence Policy, the National Defence Strategy and the National Defence White Paper are the key documents on Brazil's defence policy. The Cyber Defence Military Doctrine consolidates the key concepts and definitions regarding cyber defence in Brazil.

NATIONAL DEFENCE FRAMEWORK

Originally launched in 1996, Brazil's National Defence Policy was revised in 2005, 2012, 2016 and 2020. Similarly, the first National Defence Strategy was published in 2008 and later reviewed in 2012, 2016 and 2020. The last version of these documents spans from 2020 to 2024, at which point the Ministry of Defence will review the documents again and submit them to the federal Congress. While the National Defence Policy sets the national defence goals, the National Defence Strategy describes the strategic actions needed to accomplish such goals. Moreover, following a global trend, Brazil has also published its National Defence White Paper, which provides the country's defence vision and an analysis of the domestic and international security environment.[51]

Cyberspace was recognized as a strategic domain alongside the nuclear and outer space sectors in the 2008 National Defence Strategy. Since then, cyberspace has been discussed in these documents. The 2008 version stressed that national defence must be considered together with the country's national development strategy.[52] The National Defence Strategy highlighted the importance of technological independence, especially in the three strategic sectors (cyberspace, nuclear, and outer space) to ensure the country's defence and development. For this reason, the 2008 National Defence Strategy focused on building the country's cyber defence capacity in the three branches of the Armed Forces and ensuring interoperability among them.

The National Defence Strategy pointed out that it is crucial to invest in human capacity, as well as technological capacity, to properly defend cyberspace. The National Defence Strategy focused on improving cyber defence capacity (both technical and human) and ensuring coordination among the Armed Forces, as well as other key actors, through strategic partnerships with friendly States. Achieving technological independence is another critical component of Brazil's national defence framework. This same logic has been present in all National Defence Strategy documents since 2008.

The concerns over cyberspace and the need for technological independence are reasserted and deepened in the 2012 version of the National Defence Strategy, the National Defence Policy and the National Defence White Paper.[53] Indeed, the 2012 National Defence Strategy and National Defence Policy included a new section dedicated to the development of technological independence through the restructuring of the Defence Industrial Base (BID). The BID is composed of industries from the public and private sectors, as well as civilian and military organizations that conduct research, design, development, production and modernization of defence products in the country. In that same year, the Defence Industrial Base Law was approved to strengthen the development of defence products.[54]

To develop Brazil's BID in the cyber sector, the National Defence Strategy stressed the importance of bringing the BID closer to academia and implementing science and technology capacity-building programmes to train scientists. Owing to the multidisciplinary nature of the cyber domain, the 2012 National Defence Strategy stated that the Ministry of Defence and the Ministry of Science, Technology, and Innovation would work together to foster the BID through a two-pronged approach: (1) knowledge development and job creation and (2) development of innovative national solutions to protect strategic infrastructure. Concerning the latter, the National Defence Strategy described the use of cyber defence simulators and the development in subsequent years of artificial intelligence tools, a risk management system and an information technology certification system, as well as the creation of the National School

[51] Brazil, Ministry of Defence (2020).
[52] Brazil (2008).
[53] Brazil, Ministry of Defence (2012a); Brazil, Ministry of Defence (2012e).
[54] Brazil (2012b).

of Cyber Defence.[55] The 2012 National Defence White Paper provided more information about the different cyber defence projects undertaken within the Armed Forces, such as timelines and estimated budget.[56]

The Ministry of Defence also published the Cyber Defence Policy in 2012. Whereas the National Defence Strategy and the National Defence Policy provided guidance on national defence matters at the political level, and the white paper an overview of the security environment, the Cyber Defence Policy focused on providing guidance on cyber operations conducted at the strategic, operational and tactical levels. The 2012 Cyber Defence Policy mostly focused on ensuring the security of the major events (2012–2016). Therefore, a new cyber defence policy is needed to deal with current and future challenges. At the time of writing, Brazil has not published a new cyber defence policy.

In 2016, the new versions of the National Defence Policy and the National Defence Strategy introduced, respectively, the "defence policy concept" and the "defence strategy concept",[57] which describe the progression from diplomatic efforts to the deployment of the Armed Forces in cases of escalation from peace to crisis scenario and then to armed conflict or war. According to the defence policy concept, national security is underpinned by development, diplomacy and defence. The document recommended adopting 18 political positions in the defence field, with the first three focusing on the pacific settlement of disputes and the support of multilateralism and international organizations. The defence strategy concept also reasserted the pacific settlement of disputes. Moreover, the defence policy concept indicated the need to prioritize investment in science, technology and innovation to ensure the country's technological independence as well as budget regularity for the defence sector. The defence policy concept concluded by encouraging society's greater involvement in defence matters to develop a participative and collaborative culture in the sector.[58]

Concerning the goals and strategic actions for the cyberspace domain, the 2016 National Defence Policy and National Defence Strategy reasserted the importance of collaborating with other sectors (e.g. academia, private sector, other government agencies) and with other countries' armed forces. The development of the BID was restated.

The 2016 National Defence White Paper[59] discussed the emergence of "future conflicts" and hybrid wars, in which State and non-State actors are involved in operations of an irregular nature, particularly in cyberspace. The combination of operations of different natures are more complex and sophisticated, posing significant challenges to the Armed Forces' missions. The concept of "cyberwars" was also discussed in the 2016 white paper as one of the potential challenges of the twenty-first century. The document raised concerns about the development of information and communications technology (ICT) as military tools by some countries and pointed out the importance of the international community building an open, transparent, stable and secure cyberspace. The document highlighted the importance of Brazil's active participation in the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace.[60]

The 2020 National Defence Policy, National Defence Strategy[61] and National Defence White Paper[62] are the latest versions of these documents. As stated in 2016, the defence policy concept is based on three pillars (development, diplomacy and defence). Although the importance of diplomacy, multilateralism and international organizations are reaffirmed in the 2020 version, the first political positions are now focused on adequately equipping the Armed Forces and ensuring budget regularity for the defence sector.

Like the defence policy concept, the "strategic defence concept" underlines that budget continuity and predictability are crucial for the defence sector. Cooperation between government, private sector and academia is once again encouraged, especially to enhance the BID and ensure Brazil's technological independence in the science, technology and innovation field.[63]

The strategic defence concept reaffirms the need to seek peaceful resolutions to prevent conflicts

[55] Brazil, Ministry of Defence (2012e, 142-143).
[56] Brazil, Ministry of Defence (2012a, 202).
[57] Brazil, Ministry of Defence (2016b).
[58] Brazil, Ministry of Defence (2016b, 201).
[59] Brazil, Ministry of Defence (2016a).
[60] Brazil, Ministry of Defence (2016a, 45).
[61] Brazil, Ministry of Defence (2020d).
[62] Brazil, Ministry of Defence (2020a).
[63] Brazil, Ministry of Defence (2020d, 34).

before employing military operations.[64] The strategic defence concept also stresses the importance of the South Atlantic communication lines and the need to enhance maritime security to protect this infrastructure. To this end, the document encourages collaboration among the navies of the countries of the South Atlantic.[65]

In contrast to previous editions, the 2020 National Defence Policy highlighted the risk of crisis and conflict in Brazil's "strategic area" (South America, Antarctica, and from the Atlantic Ocean to the west coast of Africa).[66] However, this has been a gradual process. While the 2012 National Defence Policy stated that the region was "relatively peaceful", [67] the 2016 version cautioned that the stability in the region could be interrupted.[68]

The 2020 National Defence Strategy also discusses the importance of coordinating cybersecurity and cyber defence efforts, particularly in relation to critical infrastructure protection. To this end, the National Defence Strategy points out that the finalization of the Cyber Defence Military System is crucial to ensure adequate coordination between cybersecurity and cyber defence. Collaboration with academia, the private sector, the BID, and other countries' armed forces is reaffirmed in the latest version of the National Defence Strategy.[69] Also, one of its defence strategies is strengthening the country's deterrence capacity, which includes the need to increase the capabilities to defend and explore cyberspace.[70]

While the National Defence Strategy, the National Defence Policy and the National Defence White Paper define the cyber defence policy in Brazil – describing its context, goals and lines of actions – the Cyber Defence Military Doctrine defines the sector's concepts.

CYBER DEFENCE MILITARY DOCTRINE

According to the Brazilian Cyber Defence Military Doctrine, cyberspace is one of the operational domains – alongside land, sea, air and space – and activities in cyberspace can be felt in the other domains and vice versa. The doctrine defines cyberspace as the virtual space composed of computing devices where digital information transits and is processed and stored.[71]

The Cyber Defence Military Doctrine outlined the different levels of cybersecurity and cyber defence. The first level is the political level, which focuses on cybersecurity, and is led by the Presidency through the Institutional Security Cabinet (GSI). The GSI plays a regulatory role by establishing rules and procedures applied to federal public administration in relation to information security. The Brazilian Internet Steering Committee (CGI.br),[72] comprising members from government, private sector, academia and civil society, should also be involved in decisions at the political level according to the Cyber Defence Military Doctrine.[73]

The second level is the strategical level and refers to cyber defence, which is the Ministry of Defence's responsibility. Both political and strategical levels encompass cyber intelligence operations in peacetime to achieve a political or strategic goal at the highest level. At these levels, different ministries and government agencies[74] are involved, which might necessitate diplomatic efforts. Also, operations at these levels are conducted for a longer duration.

Finally, the third level includes both operational and tactical activities and focuses on cyber warfare. The Armed Forces are responsible for the activities conducted at this last level. In contrast to the political and strategical levels, the third level refers to military operations for a limited duration during conflicts. Such military operations entail previous technical and intelligence preparation. For instance, the Cyber Defence Command (ComDCiber) is considered to be between levels two and three, since it combines both strategic and operational activities.[75]

[64] Brazil, Ministry of Defence (2020d, 32).
[65] Brazil, Ministry of Defence (2020d, 33).
[66] Brazil, Ministry of Defence (2020d, 17).
[67] Brazil, Ministry of Defence (2012e, 21).
[68] Brazil, Ministry of Defence (2016b, 10).
[69] Brazil, Ministry of Defence (2020d, 60).
[70] Brazil, Ministry of Defence (2020d, 63).
[71] Brazil, Ministry of Defence (2014a, 18).
[72] CGI.br (2020).
[73] Brazil, Ministry of Defence (2014a, 25).
[74] For example, the Ministries of Defence, of Foreign Affairs, and of Science, Technology, and Innovation; the GSI; the Brazilian Intelligence Agency; and the National Telecommunication Agency.
[75] Brazil, Army (2017, 3-1).

The Brazilian Cyber Defence Military Doctrine defines cyber defence as a set of offensive,[76] defensive[77] and exploratory[78] actions carried out in cyberspace. Coordinated by the Ministry of Defence, cyber defence efforts aim to protect national information systems, gather data for intelligence purposes and compromise opponents' information systems. In the case of non-war operations, the doctrine stresses that the deployment of cyberattack actions requires explicit authorization from authorities, usually at the political level (e.g. presidency). Exploratory actions must be conducted according to the legal framework; however, the country does not have a clear legal framework about this matter.[79] Many cyber defence and intelligence aspects are defined in scattered legislation and regulated through internal administrative rules. In the case of war operations, the Cyber Defence Military Doctrine provides only some general examples, and the Joint Staff of the Armed Forces must consult with authorities at the political level to clarify the scope of its actions.

Cyberwar consists of the offensive and defensive use of information and information systems to deny, exploit, corrupt, degrade or destroy opponents' command and control capabilities in the context of a military operation. In a cyberwar, ICT tools are used to destabilize or take advantage of the opponent's ICT and command and control systems or to defend one's own ICT and command and control systems from the opponent's attacks.[80] In 2017, the Brazilian Army published the *Guideline on Cyber Warfare*, which describes only cyber warfare tactical activities.[81] In other words, it only refers to the last level of cyber defence.

As with the Cyber Defence Military Doctrine, the guideline aims to unify the concepts of cyber warfare within the Armed Forces. The guideline also describes that in a cyberwar scenario, the Joint Staff of the Armed Forces would play a key role at the operational level, and each branch (Army, Navy and Air Force) would have a cyberwar structure to carry out actions at the tactical level.[82] The guideline also acknowledges the increase in the risk of State-sponsored attacks and even smaller groups due to different motivations.[83]

The Cyber Defence Military Doctrine also acknowledges the specificities of cyber defence and cyberspace compared with traditional military defence in other domains, such as its global reach and latent insecurity, as well as the principles of effect, concealment and traceability. The principle of effect means that cyberspace actions must produce effects that can be translated into a strategic, operational or tactical advantage with an impact on the real world. The principle of concealment refers to the actions aimed at covering the origin of a cyber operation. The principle of traceability refers to the ability to detect offensive and exploratory actions involving ICT systems.[84]

The document also points out that cyber defence actions usually present a supplementary function; that is, they are not ends in themselves and are usually undertaken to support other operations. Given the different nature of cyberspace, the doctrine highlights the importance of a permanent collaboration and information exchange between government, the private sector and academia at the national and international levels.

On the one hand, by unifying cyber defence definitions, the Cyber Defence Military Doctrine enables better coordination of efforts within the Armed Forces. On the other, the doctrine does not clearly define how, and in which cases of conflict, the Armed Forces would be deployed. For example, it is not clear how the international law of armed conflict is applied in this case.[85] The Brazilian *Guideline on the Application of the International Law of Armed Conflict in the Armed Forces*[86] outlines five basic principles of the law of armed conflict: distinction, limitation, proportionality, military necessity and humanity. However, the Cyber Defence Military Doctrine does not explain how specific principles that apply to cyberspace, such as the principles of concealment and traceability, are balanced with the principles of the International Law of Armed Conflict.[87]

[76] Offensive actions consist of activities to interrupt, deny, degrade, corrupt or destroy the opponent's ICTs and systems.

[77] Defensive actions consist of actions to neutralize attacks against one's own ICT and recurring activities to enhance one's own cyber defence capacity.

[78] Exploratory actions refer to the collection of information and intelligence to obtain situational awareness of cyberspace. These activities are aimed at producing knowledge and identifying vulnerabilities and should avoid traceability.

[79] Brazil, Ministry of Defence (2014a, 24).

[80] Brazil, Ministry of Defence (2014a, 19).

[81] Brazil, Army (2017, 1-1).

[82] Brazil, Army (2017, 3-1).

[83] Brazil, Army (2017, 1-1). Another key document to understand cyber defence operational actions is the "Operational Conception of the Cyber Defence Military System"; however, this document is restricted.

[84] Brazil, Ministry of Defence (2014a, 20).

[85] Cordeiro (2016).

[86] Brazil, Ministry of Defence (2011).

[87] Cordeiro (2016, 13–14).

Cyber Defence within the Broader Cyber-Security Framework

Although the concern over the defence of cyberspace deepened in the late 2000s, information security has been in the government agenda since the early 2000s, with the creation of the federal government's first Information Security Policy.[88] In 1999, the GSI was created to assist the President in national security and defence matters, including coordinating information security activities within the government.[89]

Despite being focused on securing information within the federal executive, the GSI was also responsible for supporting the Executive Secretariat of the National Defence Council[90] in proposing regulations, policies and standards related to information security, as well as in keeping up with the information security international doctrine and technological evolution, among other topics. In 2006, the Department of Information and Communication Security (DSIC) was created within the GSI to plan and coordinate the information and communication security activities undertaken within the federal public administration.[91]

In 2010, the GSI published the *Green Book on Cybersecurity*,[92] which aimed to provide potential directives to inform the cybersecurity debate in Brazil and the development of national cybersecurity policy for the country. The Green Book addressed cybersecurity through a comprehensive lens that included political, economic and social aspects. The importance of cybersecurity education; international cooperation; critical infrastructure protection; and science, technology and innovation was also discussed in this document. Notably, the document highlighted that cybersecurity and cyber defence concepts were still in their formative stages.[93] Critical infrastructure protection was one of the fields in which cybersecurity and cyber defence were intertwined.[94]

[88] Brazil (2000).

[89] Brazil (1999b); Brazil (2001).

[90] The Executive Secretariat of the National Defence Council is the main body that advises the President on national sovereignty matters and the defence of the democratic state (Brazil, 1991).

[91] Brazil (2006).

[92] Brazil, GSI and DSIC (2010).

[93] Brazil, GSI and DSIC (2010, 19).

[94] Brazil, GSI and DSIC (2010, 40–41).

The GSI and DSIC have published several documents and guidelines in the past decade,[95] but a comprehensive national policy for cybersecurity was only recently published. Brazil's National Information Security Policy was approved in December 2018.[96] According to this policy, information security encompasses cybersecurity, cyber defence, physical security and organizational data protection. The Brazilian Information Security Glossary[97] defined information security as the actions aimed at ensuring the availability, integrity, confidentiality and authenticity of information. The glossary defines cybersecurity as the actions oriented to ensure the resilience of ICT systems against events that could compromise the availability, integrity, confidentiality and authenticity of these systems' data and services.

Therefore, in Brazil, the technical definitions of cyber defence and cybersecurity have clear differences. While the former refers to particular military actions in cyberspace coordinated by the Ministry of Defence, the latter presents a more comprehensive definition that encompasses any effort to protect information and communications systems from cyber events. Owing to this difference, cybersecurity and cyber defence are addressed in different policy documents, albeit recognizing the need for coordination between these fields. Nonetheless, the main government body responsible for cybersecurity in Brazil, the GSI, is led by military personnel.

The National Information Security Policy stated that the government must develop a specific strategy for each component of information security and associated action plans. Although the GSI is responsible for overseeing the policies, strategies and guidelines related to information security, the Ministry of Defence was assigned the responsibility to prepare the directives and procedures for cyber defence, as well as support the GSI in cybersecurity-related activities.

As a result of the National Information Security Policy, the National Cybersecurity Strategy (E-Ciber) was published in February 2020.[98] According to the E-Ciber, although the GSI is responsible for the national coordination of cybersecurity efforts, such efforts must be aligned with the cyber defence actions defined by the Ministry of Defence. Concerning national cybersecurity governance, the E-Ciber highlights the importance of delegating to a government agency the authority to formulate cybersecurity policies and propose a regulatory framework, except for cyber defence, which will be under the control of the Ministry of Defence.

Like the 2020 National Defence Strategy, the E-Ciber also acknowledges the need to better coordinate cybersecurity and cyber defence efforts, particularly in relation to critical infrastructure protection.[99] This would benefit from the publication of the National Cyber Defence Strategy and specific action plans, which have not been published yet. Nonetheless, the National Critical Infrastructure Security Policy and the National Critical Infrastructure Security Strategy, published in December 2020,[100] are key initial steps to improving coordination between the different government agencies involved in critical infrastructure protection in the country.

The Foreign Affairs and National Defence Chamber of the Government Council, which is chaired by the GSI and composed of several ministries' representatives,[101] aims to coordinate the different critical infrastructure protection efforts, including those related to cyberspace. The chamber is an advisory body to the President and is responsible for formulating foreign affairs and national defence public policies and guidelines, as well as approving, coordinating and monitoring programmes and activities whose scope is not limited to one ministry, such as actions related to defence and international cooperation, critical infrastructure protection, cybersecurity, and other foreign affairs and defence-related topics.

[95] Such as, from 2010 to 2015, the *Guide on Critical Information Security* (2010), the *Guide for Information and Communication Security Managers* (2015), and the *Cybersecurity Strategy for the Federal Public Administration* (2015).

[96] Brazil (2018b).

[97] Brazil, GSI (2019).

[98] Brazil (2020a).

[99] According to the E-Ciber, the following sectors are considered critical infrastructure: energy, transport, water, telecommunications and the financial sector.

[100] Brazil (2018a); Brazil (2020b).

[101] Brazil (2019).

The Way Forward: the Future of Brazil's Cyber Defence

In the past two decades, cyber defence capability has substantially expanded in Brazil to allow the country to promptly respond to cyberattacks and carry out cyber defence operations if needed. The country established not only several cyber defence units but also a cyber defence policy and doctrine that support research and innovation; foreign technological independence; and cross-sectoral collaboration among government, academia, and the BID. Nevertheless, budget constraints and the lack of a unified legal framework have been highlighted as some of the major issues that hamper Brazil's cyber defence agenda. Additionally, there is a need to reconsider whether the cyber defence policies implemented so far – mostly structured for the preparation for the major events – are still adequate to meet Brazil's current and future challenges.[102] The National Defence Policy and Strategy, as well as the Guideline on Cyber Warfare, highlighted the increased concern over conflicts in cyberspace and the need to prepare for such a scenario.

Despite the substantial progress in building cyber defence capacity, mainly due to the hosting of several major events, the process has been gradual, or even relatively slow. For instance, the creation of the Cyber Defence Command (ComDCiber) and the National School of Cyber Defence was originally discussed in 2012, but they were activated in 2016 and 2019, respectively. Likewise, the creation of the Cyber Defence Observatory was defined in 2014, but the project's implementation started five years later, in 2019.

The Federal Senate reached similar conclusions when analysing the budget allocated to the cyber defence sector, particularly when compared with another strategic sector: the nuclear sector.[103] In December 2019, the Senate's Commission on Foreign Affairs and National Security issued a report assessing Brazil's cyber defence national policy[104] and making a three-pronged recommendation to improve the sector. The first aspect of the recommendation referred to the immediate need to increase the budget allocated to the cyberspace sector. The report recommended that the cyber defence budget double in the subsequent three years to achieve the goals set by the Brazilian government. As indicated in the 2018

[102] Brazil, Federal Senate (2019, 13).
[103] Brazil, Federal Senate (2019, 6).
[104] Brazil, Federal Senate (2019).

management report of the Brazilian Army, there have been significant budget cuts since 2015, which have impacted the adequate implementation of several cyber defence initiatives.[105] This is probably why the need for a recurrent and predictable budget for the defence sector has been repetitively underlined in several policies and strategic documents throughout the past decade.

The second aspect of the recommendation highlighted the need to issue a cyber defence federal law. Cyber defence in Brazil is mostly regulated through administrative acts. Notwithstanding the existence of a legal framework to protect users' rights and responsibilities online (the Brazilian Civil Rights Framework),[106] the country does not have a unified legal framework for cybersecurity and cyber defence. Hence, the Senate's report strongly recommended that the executive branch propose a national cyber defence bill to amalgamate the different guidelines and directives on national cyber defence. Also, this would be an opportunity to improve cyber defence governance.[107]

Both the Ministry of Defence and the Armed Forces issue administrative acts, and such documents focus on cyber defence operation specifics and technical aspects. However, the documents do not consider overall impact on the political and international levels. For instance, although the Cyber Defence Military Doctrine clearly states that offensive operations require explicit authorization from authorities at the political level, the country would benefit from a cyber defence legal framework. This framework could clarify the decision-making process regarding cyber defence deployment and how cyber defence operations should be considered within the broader international context. Simply put, cyber defence must also be discussed through an international lens with other key political authorities in the country, defining (1) how diplomatic efforts would be applied to avoid conflict escalation and (2) when cyber defence operations would be triggered. The Chamber of Foreign Affairs and National Defence of the Government Council could play a key role in coordinating the formulation of cyber defence guidelines and policies that take into account international relations in cyberspace.

The third aspect was a recommendation addressed to the Senate itself: the creation of a subcommission within the Commission on Foreign Affairs and National Security dedicated to national cyber defence. This would better equip the Federal Congress to assess the quality (and limits) of cyber defence policies in Brazil. As discussed, most cyber defence norms are defined within the executive branch, particularly the Ministry of Defence and the Armed Forces. Although the executive branch submits the National Defence Policy and the National Defence Strategy to the Federal Congress for review every four years, these documents examine the defence sector in general. Hence, a thorough analysis of the cyber defence sector with the Federal Congress's contributions is desirable.

The Brazilian Senate's recommendations to the cyber defence sector might provide a glimpse of what comes next in the country's cyber defence agenda. At the very least, the Senate's report describes the most urgent needs of Brazil's cyber defence sector: increase in budgetary resources, a federal cyber defence law, and greater involvement of Congress in cyber defence matters. If, on the one hand, the COVID-19 pandemic has significantly impacted the country's economy, on the other, it has brought critical information infrastructure protection to attention. Also, E-Ciber, the National Critical Infrastructure Security Strategy, and the 2020 National Defence Strategy and National Defence Policy publications might contribute to the continued development of cyber defence capabilities and the formulation of a comprehensive cyber defence legal framework, especially in light of the growing concern about cyber conflicts.

[105] Brazil, Ministry of Defence (2019, 52).
[106] Brazil (2014).
[107] Brazil, Federal Senate (2019, 12).

References

Brazil. 1991. *Law No 8,183, of April 11, 1991*, provides the organization and function of the National Defence Council. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/LEIS/L8183.htm

———. 1999a. *Complementary Law No 97, of June 9, 1999*, provides the general rules for the organization, preparation, and deployment of the Armed Forces. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp97.htm

———. 1999b. Provisional Measure No 1,911-10, of September 1999, which provides the organizational structure of the Presidency of Brazil and its Ministries. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/mpv/antigas/1911-10.htm

———. 2000. *Decree No 3,505, of June 13, 2000*, establishes the Information Security Policy in the bodies and entities of the Federal Public Administration. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm

———. 2001. *The Provisional Presidential Decree No 2,216-37, of August 31, 2001*, altered the Law No 9,649, of May 27, 1998, which provides the organizational structure of the Presidency of Brazil and its Ministries. As of 14 August 2020: http://www.planalto.gov.br/CCivil_03/Leis/L9649cons.htm

———. 2005. *Decree No 5,484, of June 30, 2005*, approves the National Defence Policy. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm

———. 2006. *Decree No 5,772, of May 8, 2006*.

———. 2008. *Decree No 6,703, of December 18, 2008*, approves the National Defence Strategy. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm

———. 2010. *Complementary Law No 136, August 25, 2010*, which alters Complementary Law No 97/1999. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp136.htm#art1

———. 2012a. *Decree No 7,809, of September 20, 2012*, which altered the organizational structure of the Armed Forces. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Decreto/D7809.htm.

———. 2012b. *Law No 12,598, of March 21, 2012*, establishes rules for the procurement and development of defence product and systems. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12598.htm

———. 2014. *Law No 12,965, of April 23, 2014*, which establishes the principles, guarantees, rights, and responsibilities for the use of the Internet in Brazil. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

———. 2018a. *Decree No 9,573, of November 22, 2018*, which approves the National Critical Infrastructure Policy. As of 23 March 2021: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm

———. 2018b. *Decree No 9,637, of December 26, 2018*, approved the National Information Security Policy. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm

———. 2019. *Decree No 9,819 of June 3, 2019*, which determines the responsibilities of the Foreign Affairs and National Defence Chamber of the Government Council. As of 23 March 2021: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Decreto/D9819.htm

———. 2020a. *Decree No 10,222, of February 5, 2020*, which approves the National Cybersecurity Strategy. As of 14 August 2020: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/D10222.htm

———. 2020b. *Decree No 10,569 of December 9, 2020*, which approves the National Critical Infrastructure Security Strategy. As of 23 March 2021: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm

Brazil, Army. 2015a. *Ordinance No 001-Cmt EX, of January 2, 2015*, activated the NuComDCiber.

———. 2015b. *Ordinance No 002-Cmt EX, of January 2, 2015*, activated the NuENaDCiber.

———. 2016. *Ordinance No 004-EME, of January 8, 2016*, approved the directives for the ComDCiber project implementation.

———. 2017. *Manual de Campanha – Guerra Cibernética*. As of 15 September 2020: https://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf

———. 2019a. *Exército e Universidade Federal de Pernambuco assinam acordo para ações de defesa cibernética*. As of 14 August 2020: https://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercito-e-ufpe-assinam-acordo-para-acoes-de-defesa-cibernetica/8357041

———. 2019b. *Relatório de Gestão – Comando do Exército 2019*. As of 14 August 2020: http://www.eb.mil.br/documents/10138/11403247/RELATORIO+DE+GESTAO+DO+COMANDO+DO+EXERCITO+-+2019.pdf/5a0fd542-33cb-cb4d-5679-f1e28abe1da2

———. 2021. *Relatório de Gestão – Comando do Exército 2020*. As of 13 April 2021: https://www.eb.mil.br/testewhats?p_p_id=31_INSTANCE_sDDTov7Rur7W&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_31_INSTANCE_sDDTov7Rur7W_struts_action=%2Fimage_gallery_display%2Fview_image&_31_INSTANCE_sDDTov7Rur7W_fileEntryId=13070798

Brazil, Army Commander. 2009. *Ordinance No 03-Res, of June 29, 2009.*

———. 2010a. *Ordinance No 004-RES, of July 22, 2010*, approved the directives for the implementation of the cyber sector within the Army.

———. 2010b. *Ordinances No 666 and No 667, of August 4, 2010.*

Brazil, Federal Senate. 2014. *CPI da Espionagem. 2014. Relatório Final*. Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. Brasília: Câmara dos Deputados. As of 14 August 2020: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco

———. 2019. *Relatório de Avaliação de Política Pública – A Política Nacional sobre Defesa Cibernética.*

Brazil, Institutional Security Cabinet (GSI). 2019. *Ordinance No 93, of September 26, 2019*, which approves the Information Security Glossary. As of 14 August 2020: https://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663

Brazil, Institutional Security Cabinet (GSI) and Department of Information and Communication Security (DSIC). 2010. *Green Book on Cybersecurity*. As of 14 August 2020: http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf

Brazil, Ministry of Defence. 2009. *Ministerial Directive No 0014, of November 9, 2009.*

———. 2011. *Manual de Emprego do Direito Internacional dos Conflitos Armados (DICA) nas Forças Armadas*. As of 14 August 2020: https://bdex.eb.mil.br/jspui/bitstream/123456789/140/1/MD34_M03.pdf

———. 2012a. *Livro Branco de Defesa Nacional*. As of 14 August 2020: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/livro_branco/livrobranco.pdf

———. 2012b. *Normative Ordinance of the Ministry of Defence No 2,221, of August 20, 2012*, approves the Ministerial Directive that establishes guidelines for the Ministry of Defence's activities included in the Major Events determined by Presidency of the Republic. As of 14 August 2020: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=2270&ANO=2012&SER=A

———. 2012c. *Normative Ordinance of the Ministry of Defence No 3,389, of December 21, 2012*, approves the Cyber Defence Policy. As of 14 August 2020: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3389&ANO=2012&SER=A

———. 2012d. *Ordinance No 3,405, of December 21, 2012*. As of 14 August 2020: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=3405&ANO=2012&SER=A

———. 2012e. *Política Nacional de Defesa / Estratégia Nacional de Defesa*. As of 14 August 2020: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf

———. 2013. *Ordinance No 2,569/EMCFA/MD, of September 6, 2013*, created the Cyber Defence Working Group for the purpose of recommending measures to enhance Brazil's cyber defence capacity.

———. 2014a. *Doutrina Militar de Defesa Cibernética*.

———. 2014b. *Normative Ordinance of the Ministry of Defence No 2,777, of October 27, 2014*, establishes the directives for measures to enhance Cyber Defence. As of August 2020: https://mdlegis.defesa.gov.br/norma_pdf/?NUM=2777&ANO=2014&SER=A

———. 2014c. *Ordinance of the Ministry of Defence No 3,010/MD, of November 18, 2014*, approves the Cyber Defence Military Doctrine. As of 14 August 2020: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf

———. 2016a. *Livro Branco de Defesa Nacional*. As of 14 August 2020: https://legis.senado.leg.br/sdleg-getter/documento?dm=5068932&ts=1594035319440&disposition=inline

———. 2016b. *Política Nacional de Defesa / Estratégia Nacional de Defesa*. As of 14 August 2020: https://legis.senado.leg.br/sdleg-getter/documento?dm=5068932&ts=1594035319440&disposition=inline

———. 2019. *Relatório de Gestão do Exército Brasileiro – Exerício 2018*. As of 14 August 2020: http://www.cciex.eb.mil.br/images/pca/2018/cmdopca2018.pdf

———. 2020a. *Livro Branco de Defesa Nacional – Brasil 2020*. As of 14 August 2020: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf

———. 2020b. *Ordinance No 3,781/GM-MD, of November 17, 2020*, which establishes the Cyber Defence Military System (SMDC). As of 23 March 2021: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860

———. 2020c. *Plano de Articulação e Equipamento de Defesa*. As of 14 August 2020: https://www.gov.br/defesa/pt-br/assuntos/industria-de-defesa/paed/plano-de-articulacao-e-equipamento-de-defesa-paed

———. 2020d. *Política Nacional de Defesa / Estratégia Nacional de Defesa*. As of 14 August 2020: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf

Brazil, Presidency. 1996. *Política de Defesa Nacional*. As of 14 August 2020: http://www.biblioteca.presidencia.gov.br/publicacoes-oficiais/catalogo/fhc/politica-de-defesa-nacional-1996.pdf

Center for Security Studies (CSS). 2019. 'Trend Analysis – Cybersecurity at Big Events.' *CSS Cyber Defence Project*. As of 13 April 2021: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-11-Cybersecurity-at-Big-Events.pdf

CGI.br. 2020. *About CGI.br*. As of 14 August 2020: https://www.cgi.br/about

Cordeiro, Luis Eduardo Pombo Celles. 2016. 'Análise da Doutrina Militar de Defesa Cibernética a Luz do DIH/DICA.' *IX Encontro Nacional da Associação Brasileira de Estudos de Defesa*.

Costa, Alan Denilson Lima. 2013. 'O Setor Cibernético no Exército Brasileiro e suas Consequências Doutrinárias no Recrutamento de Pessoal no Exército Brasileiro.' *Revista do Exército Brasileiro* 149: 62–78. As of 14 August 2020: https://en.calameo.com/books/001238206530442dcc28b

DefesaNet. 2012. *MD – Governo aprova Política de Defesa Cibernética*. As of 14 August 2020: https://www.defesanet.com.br/cyberwar/noticia/9129/MD---Governo-aprova-Politica-Cibernetica-de-Defesa

DefesaTV. 2019. *Exército Brasileiro ativa sua Escola Nacional de Defesa Cibernética*. As of 14 August 2020: https://www.defesa.tv.br/exercito-brasileiro-ativa-sua-escola-nacional-de-defesa-cibernetica

Escola Superior de Guerra. 2016. *Ciberdefesa e cibersegurança: novas ameaças à segurança nacional.* Rio de Janeiro: ESG.

SegInfo. 2014. *Ministéiro da Defesa cria o Comando de Defesa Cibernética*. As of 14 August 2020: https://seginfo.com.br/2014/11/10/ministerio-da-defesa-cria-o-comando-de-defesa-cibernetica-2

Tanji, Thiago. 2012. 'Como o exército protege o espaço virtual brasileiro.' Exame, 16 July 2012, 10.07 p.m. As of 14 August 2020: https://exame.com/tecnologia/como-o-exercito-protege-o-espaco-virtual-brasileiro

Building Cyber Operational Capabilities:

Brazil's Efforts over the Past Two Decades

This paper describes the evolution of cyber defence in Brazil, from early discussions in the 2000s to specific policies and measures implemented to develop the national capability to conduct international cyber operations if necessary. Although Brazil has been strengthening its cyber defence capacity for the past two decades, the major international events hosted by the country from 2012 to 2016, such as the World Cup and the Olympic Games, marked a watershed in Brazil's cyber defence capacity development. During this period, not only did Brazil solidify its cyber defence military structure, it also developed a cyber defence doctrine aimed at unifying concepts and guiding operations in cyberspace.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH