ARTICLE DOI 10.52781/cmm.a196

CYBEROS system and its vertical of tactical radio network: reflections on potential contributions to national defense

El sistema CYBEROS y su vertical de redes de radios tácticos: reflexiones sobre las posibles contribuciones a la Defensa Nacional

Abstract: Normative documents that define policies and guiding strategies for Brazilian national defense and its various branches highlight the importance of the cyber sector. Strengthening it involves several strategies, such as integrating academia with the defense industrial base, developing dual-use technologies, and training specialized human resources. In this context, the CYBEROS system stands out as an innovative computational tool that offers cybersecurity exercises by realistically simulating critical infrastructure protection scenarios and tactical radio networks. This study reflects on the potential contributions of this tool to national defense, especially regarding the cyber sector. For this, a qualitative study was conducted comparing strategic actions in the current normative framework with the main expected outcomes of this development. The findings indicate that CYBEROS and its vertical of tactical radio networks directly contribute to several of these strategic actions.

Keywords: Cyber defense; Tactical communications; Software-defined radio; National Defense; Critical infrastructure protection.

Resumen: Los documentos normativos que definen las políticas y estrategias rectoras de la Defensa Nacional y de varias de sus ramas destacan la importancia del sector cibernético. El fortalecimiento de este sector pasa por varias estrategias específicas, como la integración del ámbito académico con la base industrial de defensa, el desarrollo de tecnologías de doble uso y la capacitación de recursos humanos especializados. En este contexto, destaca el sistema CYBEROS, una herramienta computacional innovadora que permite realizar ejercicios de ciberseguridad mediante la simulación realista de escenarios de protección de infraestructuras críticas, así como de redes de radios tácticos. Este trabajo presenta reflexiones sobre las posibles contribuciones de esta herramienta a la Defensa Nacional, con énfasis en el sector cibernético. Para ello, se realizó una investigación cualitativa en la que se compararon las acciones estratégicas previstas en el marco normativo actual con los principales resultados esperados de ese desarrollo. Se constata que CYBEROS y su vertical de redes de radios tácticos contribuyen de manera objetiva a varias de esas acciones estratégicas.

Palabras clave: Ciberdefensa; Comunicaciones tácticas; Radio definida por software; Defensa nacional; Protección de infraestructuras críticas.

Maurício Henrique Costa Dias
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ)
Rio de Janeiro, RJ, Brasil
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
mauricio.dias@cefet-rj.br

George Alex Fernandes Gomes
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
george.gomes@ime.eb.br

Danilo Habermann
Exército Brasileiro (Cel Veterano)
Campinas, SP, Brasil
danilo.habermann@gmail.com

Paulo César Pellanda
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
pellanda@ime.eb.br

Juraci Ferreira Galdino
Instituto Militar de Engenharia (IME)
Rio de Janeiro, RJ, Brasil
galdino@ime.eb.br

Received: Aug. 27, 2025
Accepted: July 29, 2026

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
https://colecaomeiramattos.com.br/CMM

Creative Commons Attribution Licence

1 INTRODUCTION

The National Defense Policy (NDP) and the National Defense Strategy (NDS) constitute the highest unclassified guiding documents in Brazilian national defense (Brasil, 2024a). The NDP describes the basic Brazilian assumptions regarding its defense and establishes the national defense objectives (NDO). In turn, the NDS guides all segments of the Brazilian State on the measures to be implemented to achieve objectives, defining defense strategies (SD) and strategic defense actions (SDAs).

An important highlight in this documentation is the need to strengthen the three strategic technological sectors in national defense: nuclear, space, and cyber (Brasil, 2024a); this document also attributes each of these sectors to a branch of the armed forces (AF; i.e., navy, air force, and army, respectively), considering the matrix of these sectors between the three AF. This composition of strategic technological sectors and their respective responsibilities are the same as those originally provided for in the first edition of the NDS (Brasil, 2008).

Of these three sectors, the cyber has the most incipient technological maturity and the capacity to most broadly permeate all three AF. It comprises a set of technologies, processes, and practices designed to protect networks, computers, programs, and data from attacks, damages, or unauthorized access. This sector is essential for national security and defense as cyber threats can compromise critical infrastructures (CIs) such as energy, communications, and defense systems. Cyber defense involves implementing preventive and reactive measures to detect, respond to, and neutralize threats, ensuring the integrity, confidentiality, and availability of national strategic information and systems.

In fact, CI protection from the cyber sector point of view is a global concern from the beginning of the 21st century that has demanded increasing attention, as warned by Pinheiro (2008), Sandoval (2020), and Souza, Oliveira, and Paula (2024), with evident impact to contemporary military doctrines. Since then, many discussions have developed regarding the cyber sector, CI protection, and other related ramifications in the national defense of Brazil and other nations. Recent examples of these contributions occur in Medeiros, Carvalho, and Goldoni (2019); Malagutti (2022); Castilho (2023); Okabayashi (2024); and Schwether (2025).

The current importance and dimension of the cyber sector are such that care for it must go beyond the Ministry of Defense. The National Cybersecurity Policy (PNCiber) (Brasil, 2023) and the National Cybersecurity Strategy (E-Ciber) (Brasil, 2025) stand out in this broader context. Following the same line of reasoning, CI protection has also gained broader projection and high-level normative legislation with the formulation of the National Policy for the Security of Critical Infrastructures (PNSIC) (Brasil, 2018a) and the National Strategy for the Security of Critical Infrastructures (ENSIC) (Brasil, 2020b).

The expected role of Brazilian academia grows in importance in its primary function of training human resources or in conducting research, development, and innovation (RD&I) to integrate the public and private productive segments, especially regarding the defense industrial base. As shown throughout this normative framework, this is one of the main paths in the search for cyber technological innovations (preferably dual-use ones) that

help Brazil to achieve technological autonomy and strengthen its position in the current and future global geopolitical scenario (Barbosa; Caldeira, 2021; Moreira; Galdino, 2024).

An example of an academic environment that can help to fulfill the expected contribution to this context is the Cybersecurity Laboratory of Cyberphysical Systems (LaSC) at Instituto Militar de Engenharia (IME), commissioned at the end of 2021 (Camargo *et al.*, 2022). The LaSC infrastructure offers real-time hardware-in-the-loop simulations of cyber-physical systems under real malware attacks, enabling studies and research in cybersecurity, such as the system in Vu *et al.* (2024), for example.

At the end of 2022, a development project signed between the Funding Authority for Studies and Projects; the Brazilian Army Research, Development, and Innovation Support Foundation; the Army Technological Center, and IME called "*Inovações Tecnológicas para Segurança Cibernética de Sistemas Ciberfísicos Aplicadas a Infraestruturas Críticas e Comunicações Estratégicas e Táticas*" (ITSC2ICCOM – Technological innovations for cybersecurity of cyber-physical systems applied to critical infrastructures and strategic and tactical communications) aimed to improve the capabilities of cybernetic studies and expand the LaSC scope, incorporating new cases of use (or "verticals") representing CIs in the electrical, oil and gas, communications, and other sectors (FAPEB, 2022). After a strategic partnership selection (FAPEB, 2025) in which the Telecommunications Research and Development Center was the contracted institution, the most significant development of this project began in 2025: the CYBEROS system, a national cyber range (Lillemets *et al.*, 2025) customized to realistically simulate real networks, systems, and infrastructures. It offers education and typical training exercises in cybersecurity, bringing in innovative virtualized environments for realistic simulations of CI protection scenarios and military communications networks.

The vertical that gained the most initial attention was that of tactical radio networks, composed of devices such as those in the defense software-defined radios (SDR) family, the development of which has involved several defense industrial base members for more than a decade (Branco *et al.*, 2014; Redação Tecnologia & Defesa, 2024). The justification of this priority stems from the fact that the advent of cybersecurity doctrines has added new concerns about the vulnerability of these networks in addition to those provided for by the military doctrines of communications and electronic warfare, as exemplified by the mapping of attack classes on tactical SDR in Silva, Moura, and Galdino (2012) and the methodology in Kloth *et al.* (2024).

Hence the research problem in this study: how can CYBEROS and its verticals (especially that of tactical radio networks) contribute to Brazilian national defense? This study aims to show that the potential contributions of this development and its context are aligned with the main guiding documents on national defense policies and strategies, especially in the cyber sector. For this, this study carried out qualitative research focused on the high-level normative framework supporting national defense in search of objectives, strategies, and strategic actions in line with CYBEROS.

Section 2 better details LaSC and ITSC2ICCOM, which includes the CYBEROS system and its verticals. Section 3 describes the methodology in this study. Section 4 details the alignment of the system with the main pertinent national defense policies and strategies. Section 5 reflects on the potential contributions of the chosen tactical radio network vertical. Section 6 concludes this study.

2 LASC AND ITSC2ICCOM

2.1 History and background

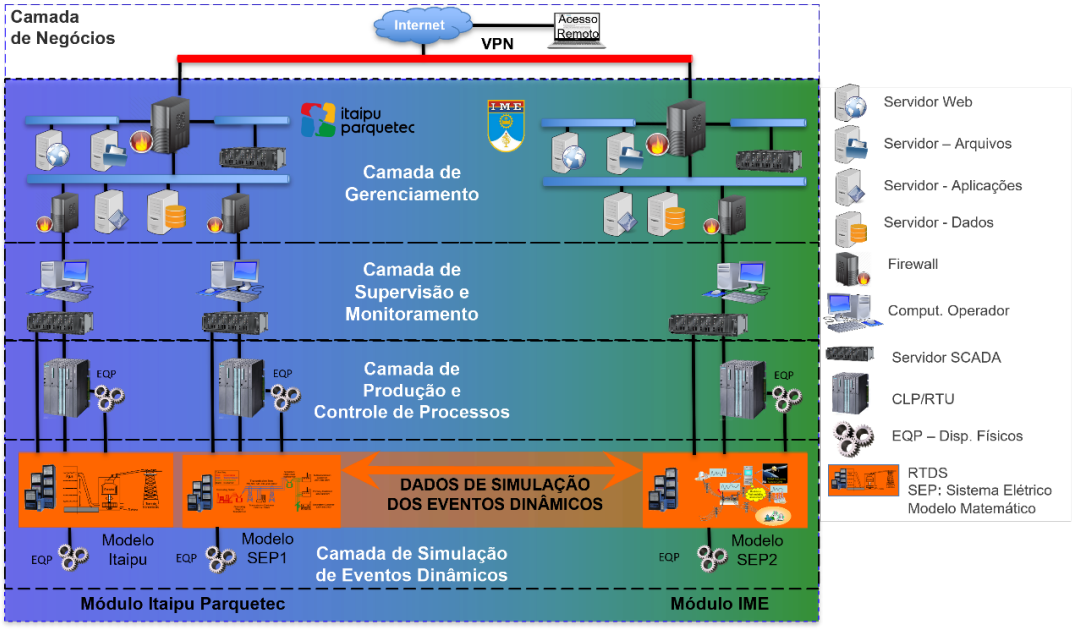
The economy and society deeply depend on information and communication technologies, making the cyberspace a critical domain interfering in the economic, social, and political spheres of states and requiring the adaptation of security doctrines and strategies. This dependence brings growing vulnerabilities and threats, such as phishing, denial-of-service attacks, data leakage, espionage, and cyber terrorism. The indiscriminate dissemination of information online, including scripts for launching cyberattacks, enables increasingly sophisticated attacks from users requiring no high technical knowledge; hence the constant threat to information confidentiality, integrity, authenticity, and availability. This context includes concerns regarding cyberattacks against CI services, the interruption or destruction of which can cause serious impacts, compromising the security of the state and society (Cravo, 2023; Fontes, 2024; Gomes; Laginestra, 2023; Melo; Albuquerque; Mendonça, 2022; Reis, 2024; Santos Junior *et al.*, 2019).

The creation of LaSC met this concern, supporting RD&I in electricity CI cybersecurity by real-time hardware-in-the-loop simulations involving integrated models and devices of electrical networks (generation, transmission, and distribution) and of information, communication, and automation technologies that faithfully represent real system behavior (Figure 1). These simulations at the initial phase of LaSC involved the application of real cyber events (attacks of varied nature), focusing on malware and the cyber contamination of industrial environments to assess their effects on the layers, find vulnerabilities, and propose solutions.

In its relatively short existence, LaSC has accumulated significant scientific, technological, and innovation capacity in cybersecurity, with important results in supporting the training of human resources and intellectual production. In this context, the creation of the Graduate Course in Protection of Electrical Systems in 2022 (IME, 2025) deserves mention. LaSC also began to contribute to research at IME *stricto sensu* graduate courses.

Another vector of the LaSC contribution refers to its support to the preparation and composition of Brazilian military teams to participate in national and international cyber exercises. The May 2024 Cyber Flag (Barros, 2024) and June 2025 Cyber Shield (Barros, 2025)—coordinated by the United States Cyber Command and the United States Department of Defense (considered the largest cyber combat exercises in the world)—stand out. On both occasions, a month before these exercises, a LaSC team provided training on specific cybersecurity issues on CI protection to the military personnel of the three AF that made up the Brazilian teams. LaSC contributed to planning, participating in the 2024 Cyber Guardian Exercise (it was also to participate in its 2025 edition). The Cyber Guardian Exercise is the largest cyber defense exercise in the southern hemisphere. Organized by the Cyber Defense Command (Brasil, 2024b), it involves public and private sectors related to CI protection in Brazil.

Figure 1 — LaSC: initial logical conception of experiments and simulations



Source: LaSC members (2021).

After being commissioned, the preliminary results pointed to the potential contributions by LaSC in RD&I and in the training of human resources much broader than the initial scope, mainly linked to the electricity CI protection. To expand the laboratory activities and give more projection to its results, IME sought funding from the Funding Authority for Studies and Projects in partnership with the Army Technological Center and the Brazilian Army Research, Development, and Innovation Support Foundation, entering into an agreement to develop the ITSC2ICCOM (FAPEB, 2022). The project aims to obtain technological innovations in cybersecurity regarding cyber-physical systems applied to CI protection and strategic and tactical communications. The development of these innovations focuses on applications in SDR and communications systems for military and civilian use and other cyber-physical systems.

2.2 System CYBEROS

After a period of maturation regarding premises, methodology, objectives, and requirements, the demands for the most significant contribution expected from the ITSC2ICCOM project—the CYBEROS system—were established. This system is developed in partnership with the Telecommunications Research and Development Center, the winning institution of the public notice launched in early 2025 (FAPEB, 2025).

CYBEROS performs the automated orchestration of cybersecurity scenarios, enabling training and exercises typical of this context—such as the well-known capture the flag model (Švábenský *et al.*, 2021)—in virtualized environments of realistic simulations. An innovation in this conception is the integration of complementary modules to what would be the typical core of a cyber range, which enables the operation of the verticals in specific CI protection scenarios.

Such a solution may fill gaps LaSC found due to the increasing sophistication and frequency of attacks targeting strategic sectors. Platforms such as Hack The Box[1] and TryHackMe[2] are neither fully customized for specific aspects of CI protection scenarios nor can fully customize scenarios, rendering CYBEROS as an innovative and strategic solution.

Figure 2 illustrates the initial conceptual architecture of CYBEROS. It is modular, scalable, and compatible with the existing LaSC environment, including the use of tools similar to OpenStack (Adiwal; Misbahuddin, 2023) as pillars for virtualization and orchestration. It is based on three main modules: frontend, orchestrator, and backend. Frontend is the graphical interface accessible to users, designed to facilitate interaction with the system, enabling the configuration of cyber scenarios and topologies, real-time monitoring of the progress of the exercises, and the visualization of performance metrics.

The core of CYBEROS is its orchestrator; it automates the creation, configuration, and execution of simulated scenarios, operating on a cloud computing platform equivalent to OpenStack, with functionalities that include virtual machine and container management (Tang, 2025), automated configuration of simulated networks and devices, support for integration with physical devices (including hardware-in-the-loop formats), and continuous monitoring of the state of scenarios and resource allocation. In turn, backend processes user requests and integrates them into the system. Its features include user and permission management, logging and system activity reports, and integration with databases for secure and efficient storage.

Virtualization is a way to encapsulate and isolate cyber challenges, ensuring a consistent and secure environment for cyber exercise participants. The orchestrator is essentially the cloud operating system that manages and orchestrates virtual machines and/or containers, as well as the associated network and the large-scale storage infrastructure. This strategy permeates the infrastructure of larger, more complex exercises such as modern capture-the-flag models, creating, managing, and isolating the environments hosting cyber challenges.

An important requirement of the system is the adoption of open-source tools without modifying them (Feller *et al.*, 2005). Any change must take place via an application programming interface (Bagga, 2023). The system must also be compatible with security information and event management tools (Conti *et al.*, 2018) and with continuous malware monitoring or dynamic analysis tools (Or-Meir *et al.*, 2019) for data exploration and visualization and to be able to track the health of servers and find anomalous behavior.

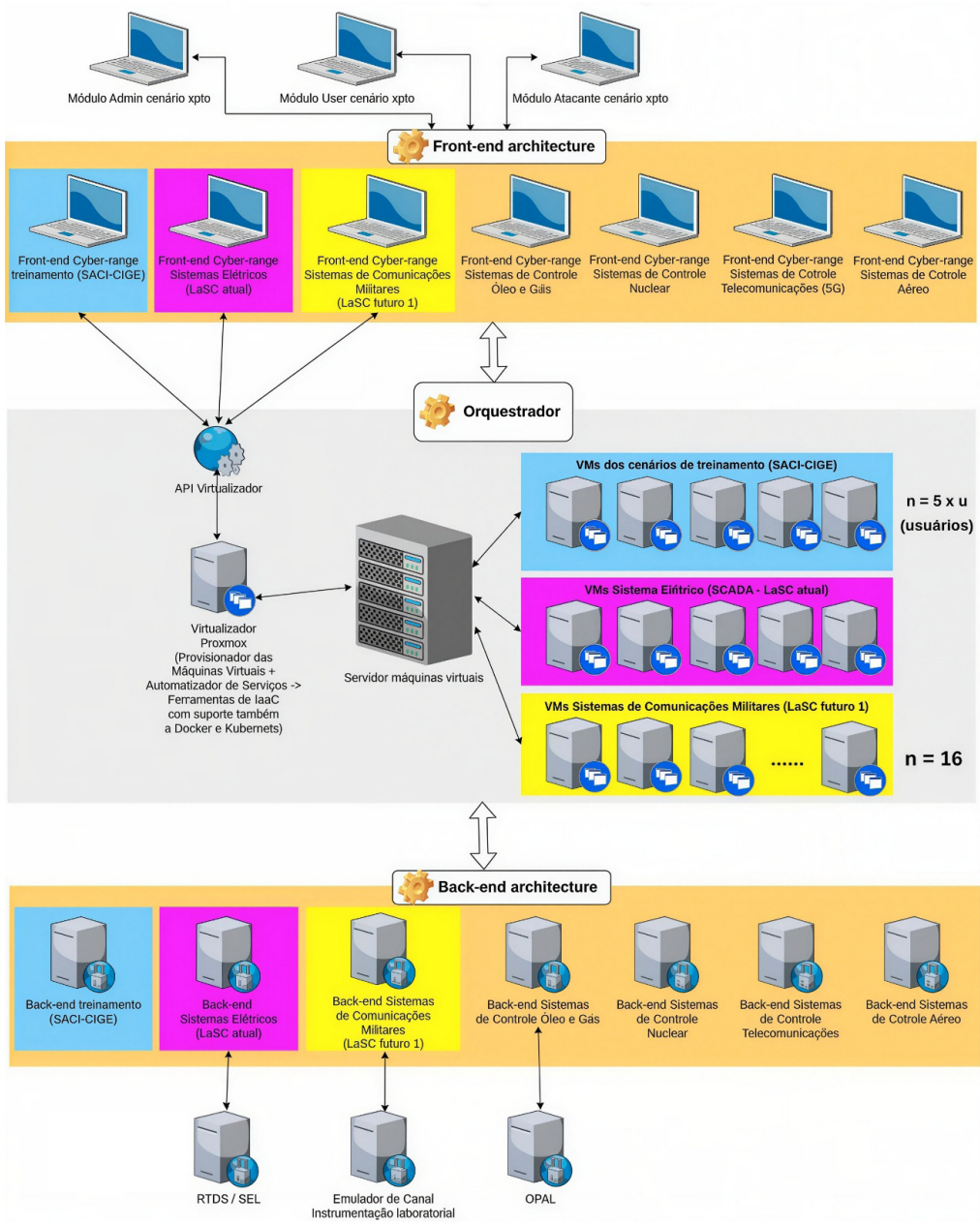
Figure 2 helps to understand the concept of CYBEROS-integrated verticals. Rather than an exact module, a vertical only represents the execution of a cybersecurity exercise simulation case or scenario and its peculiarities. This mask portrays the vision and needs of a specific user profile of CI protection scenarios. For example, the elements in magenta in Figure 2 represent the

1 Available at: https://www.hackthebox.com/. Access on: Aug. 12, 2025.

2 Available at: https://tryhackme.com/. Access on: Aug. 12, 2025.

use of CYBEROS complemented by integrated modules supporting cybersecurity exercises in an electricity sector scenario, characterizing the electricity sector vertical.

Figure 2 – Initial conception of the CYBEROS architecture



Source: LaSC members (2024).

By integrating resources that can execute cyber exercises in realistic CI protection scenarios in a vertical, the very availability of this virtualized scenario and integration to hardware-in-the-loop elements adds another application for the tool: the exploration of performance aspects and simulations of using the system in a vertical. The effective use of this potential involves integrating

additional complementary modules with CYBEROS, the specificities of which vary according to the vertical. In particular, the development of this initial version of CYBEROS offered this mode of performance analysis for a military communication system vertical or, more specifically, for tactical radio networks mainly composed of SDR. Such use of verticals represents an alternative for training or operational exercises in closed and controlled environments, which could support the training of troops and generate new knowledge of interest to the doctrine.

2.3 Tactical Radio Networks Vertical

Military tactical communication systems also suffer cyberattacks and, as such, need robust protection (Al-Shara; Ahmad, 2018; Heinäaro, 2015; Reis, 2024; Sneps-Sneppe, 2024). The electromagnetic spectrum has become a highly contested battleground. Its operational requirements demand specialized tactical communication infrastructures that can ensure seamless connectivity and secure information exchange even under adverse conditions (Kloth *et al.*, 2024; Thomas; Fiala, 2020). SDR, components widely present in current tactical radio networks (Bergstrom *et al.*, 2002), offer remarkable functional flexibility and significantly expand the cyberattack surface due to their reliance on logical components and software layers. SDR vulnerabilities also include risks associated with the mostly foreign hardware and software supply chain, reliance on remote updates, and the use of potentially compromised open-source libraries (Baldini *et al.*, 2012; Li *et al.*, 2018; Silva; Moura; Galdino, 2012, 2014).

The tactical radio network vertical integrates CYBEROS as a module compatible with the SDR-defense family. For strategic reasons, this integration was initiated by a vehicular platform for tactical communication in military vehicles and vessels to be later extended to other types of radio as they become available (FAPEB, 2025). The vehicle SDR-defense features a proprietary radio frequency module adherent to the transceiver facility specification of the SCA version 2.2.2, and the processing module, which implements an architecture in red and black, physically separated processing cores interconnected by a safety module (Branco *et al.*, 2014). With these modules, it provides a framework for executing multiple waveforms, each employing communication protocols tailored to diverse operational scenarios (FAPEB, 2022).

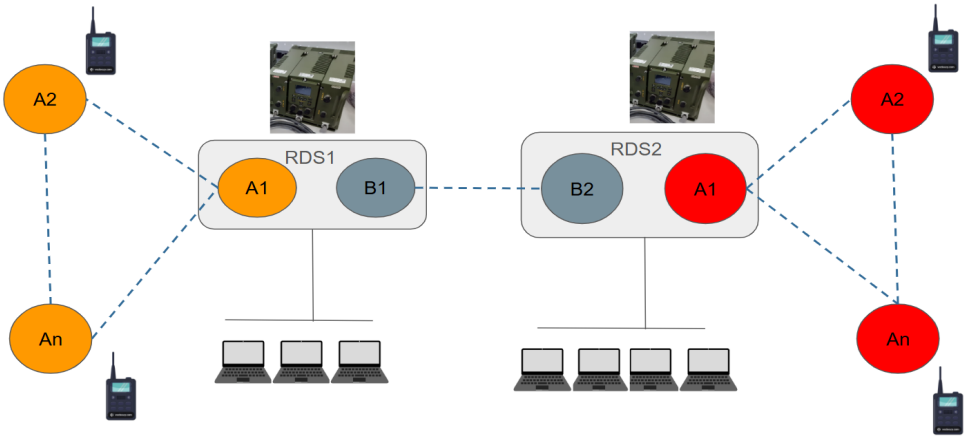
Figure 3 shows a representative use case of that vertical. The orange and red radio networks can, for example, serve two physically distant battalions, respectively. Interconnecting these networks, these vehicular SDR can simultaneously run two independent waveforms, being useful for integrating distinct networks.

The radio network in Figure 3 and other communication topologies can be fully configured in CYBEROS. In this structure, the processing modules (MP)—virtualized instances on servers—execute the waveforms on processors emulated by virtual machines. Despite processing virtualization, the transmission and reception of radio frequency signals occur through commercial physical radios, such as universal software radio peripherals[3] (USRP) or similar devices. These pieces of equipment offer great operation flexibility, with wide coverage of frequencies and bandwidths,

3 Available at: https://www.ni.com/en/support/downloads/drivers/download.ni-usrp.html. Access on: Aug. 12, 2025.

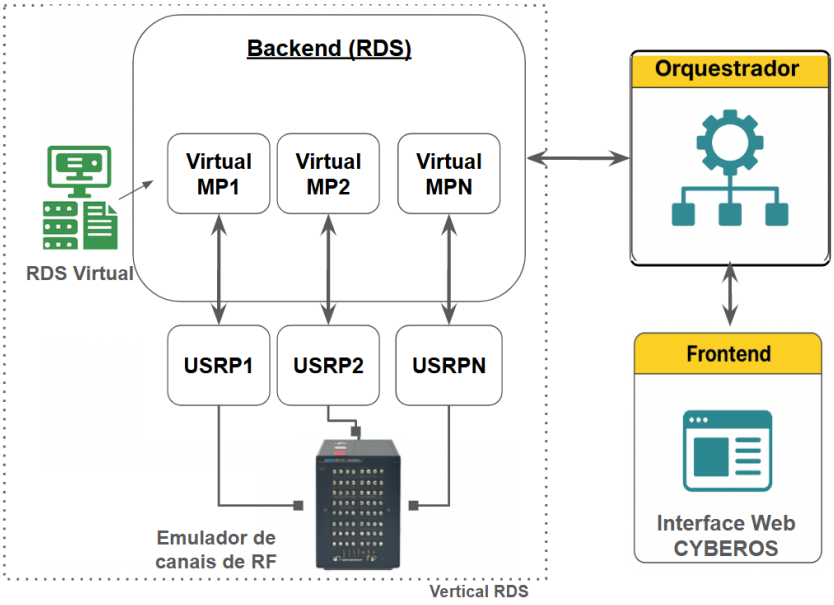
being suitable for civil applications (such as 4G, 5G, and 6G networks) and tactical scenarios. Figure 4 details this architecture, generically identifiable as one of the verticals in Figure 2 (military communications systems – yellow blocks), pointing out the use of the universal software radio peripheral and the radio frequency channel emulator. The latter is capable of applying controlled degradations to the signals exchanged among the different network nodes, such as attenuation, fading, and noise. This enables performance, interoperability, and resilience tests of waveforms under conditions equivalent to those in the field but within a controlled laboratory environment.

Figure 3 — Example of a network use case of tactical radios using SDR



Source: The authors (2025).

Figure 4 – CYBEROS virtualized SDR-based tactical radio network vertical



Source: The authors (2025).

3 METHODOLOGY

A qualitative research methodology was adopted in this study to contribute to its research problem. Qualitative research generally aims to deeply understand phenomena, exploring subjective and contextual aspects and using methods such as interviews, focus groups, and content analysis (Lakatos; Marconi, 2017). Content analysis of high-level normative documents focused on the planning of national defense and other bibliographic references pertinent to the chosen theme were chosen in search of correlations that would show how a technological innovation tool such as CYBEROS (especially operating its vertical of tactical radio networks) could objectively contribute to national defense.

Analysis was limited to three normative document groups in view of the technological context of the chosen technological innovation (cyber sector). Thus, the NDP and the NDS were analyzed in this study as the highest normative documents. PNCiber and E-Ciber were considered regarding the more specific scope of the cyber sector. Moreover, CI protection was evaluated in this study considering the PNSIC and ENSIC. Analysis focused on such political and strategic normative alignment is presented in section 4, pointing out objectives, tactics, and strategic actions that are notably met by CYBEROS as a whole and/or considering some of its verticals.

Section 5 focuses on the potential contribution of the tactical radio network vertical. Those reflections sought to complement the alignments with the high-level normative documents identified for CYBEROS as a whole and point out tactical or operational contributions.

4 ALIGNMENT WITH THE MAIN POLICIES AND STRATEGIES RELATED TO NATIONAL DEFENSE

4.1 NDP/NDS

The NDP constitutes the highest-level conditioning document for planning national defense actions. Focused primarily on external threats, it establishes eight NDO to prepare and use all expressions of the national power in favor of national defense. In turn, the NDS defines tactical strategies and actions that should guide Brazilian society in actions to defend the homeland. The current version provided for 17 SD and 85 SDAs. Some SD occur in several NDO, just as SDAs do in several SD (Brasil, 2024a).

The description of the strategic conception of defense in the NDS includes an important highlight that is directly related to this study: the governmental and industrial sectors and the academic environment, focused on science, technology, and innovation, should be prioritized and integrated to ensure that critical national technologies meet the needs of defense products. The NDS also indicates that such technologies must be obtained by synergistically stimulating and fostering industry and academia. It also indicates that defense industrial base training, including the mastery of dual-use technologies, is essential to supply defense products toward the technological autonomy of Brazil. The development

of CYBEROS fits into all these premises behind the conception of the NDS given the participation of IME, the Army Technological Center, and the Telecommunications Research and Development Center (a strategic defense company) and the dual nature of the system.

National defense capabilities (NDCs) stand out among the NDS foundations (considered those composed of portions of national power expressions). The current NDS is based on nine NDCs: Protection, Prompt Response, Deterrence, Coordination and Control, Information Management, Logistics, Strategic Mobility, Mobilization, and Defense Technological Development. Of these, two are associated with the CYBEROS system and its verticals: Protection and Defense Technological Development.

The Protection NDC expresses the most relevant NDO: guaranteeing sovereignty, national heritage, and territorial integrity. Strengthening this NDC requires adapting and structuring surveillance systems in areas of interest and control, including cyberspace. The CYBEROS system can indirectly contribute to this NDC, protecting and monitoring cyberspace, helping to train specialized personnel, and enabling studies and research on CI cyber vulnerabilities, which can guide stakeholders in decision-making processes that seek to adapt and structure surveillance systems in this strategic space.

In turn, the Defense Technological Development NDC develops and/or modernizes defense products via integrated and synergistic actions via the state, industry, and academia toward technological updating and independence. By its nature, CYBEROS fits into this context, directly contributing to this NDC.

The NDS pillars also address the defense sector, distinguishing the role of the three AF and three strategic technological sectors. The AF explicitly concern themselves with the cyber sector, especially the army, which has a centralized leadership role in it. Regarding the cyber sector, the NDS states that training should prioritize communication technologies between AF units to ensure their interoperability and ability to safely act in an integrated manner to improve information and communications security and cybersecurity at all levels of the state, focusing on CI protection. This requires fostering RD&I focused on dual technologies that can plan and execute cyber defense activities and contribute to national cybersecurity together with the academic community. Moreover, the collaborative action between the defense sector, the national academic community, the public and private sectors, and the defense industrial base should be strengthened. CYBEROS fits into these fundamental aspects underpinning the NDS.

Table 1 lists the NDO, SD, and SDAs to which CYBEROS directly or indirectly contributes. The justification for this alignment stems from an analysis of the relationship with the SDAs since meeting them also meets SD and OND. Starting with SDA 1, CYBEROS constitutes a strategic defense development in the cyber sector. Regarding SDA 2, the unique role of the CYBEROS CI protection and tactical radio network verticals contributes to the training of specialized personnel and to the availability of realistic simulations of cyber-attack scenarios,

configuring an indirect gain to increase CI security. This same line of reasoning applies to SDA 10, albeit in a limited way, as CYBEROS can help to develop capabilities to monitor and control cyberspace. Its contribution to SDA 11 can also stem from these arguments, especially regarding its ability to exploit cyberspace. Finally, its contribution to SDA 52 is self-evident and requires no further justification.

Table 1 – Alignment of CYBEROS with the NDP and the NDS

NDO	SD	SDA
I – To guarantee sovereignty, the national heritage, and territorial integrity	1 – To strengthen the national power	1 – To develop strategic defense sectors (nuclear, cyber, and space) 2 – To contribute to the increase in CI security in water collection, treatment, and distribution systems; electricity generation and distribution; transportation; fuel production and distribution; communications, among others
	2 – To strengthen deterrence capacity	10 – To develop the capabilities to monitor and control airspace, cyberspace, territory, Brazilian jurisdictional waters, and other areas of interest 11 – To increase the capabilities to defend and exploit cyberspace
III – To promote technological and productive autonomy in defense	9 – To strengthen defense science and technology	52 – To promote the development of cyber technology
VIII – To increase the projection of Brazil in the concert of nations and its insertion in international decision-making processes	1 – To strengthen the national power	1 – To develop strategic defense sectors (nuclear, cyber, and space) 2 – To contribute to the increase in CI safety in water collection, treatment, and distribution systems; electricity generation and distribution; transportation; fuel production and distribution; communications, among others

Source: The authors (2025).

4.2 PNCiber and E-Ciber

In 2018, Decree no. 9,637 published the National Information Security Policy (Brasil, 2018b). It established cybersecurity, cyber defense, physical security, and organizational data protection objectives and means to achieve them. The National Information Security Policy provided for its achievement via the National Information Security Strategy and national plans. In turn, it foresaw that that Strategy would be built in five modules with strategic actions and objectives related to information security (in line with public policies and federal government programs). These modules should address cyber security, cyber defense, CI security, security of confidential information, and data leakage protection.

The cybersecurity module was developed and published in 2020 as E-Ciber (Brasil, 2020a). It was the manifested guidance of the federal government to Brazilian society on the cybersecurity main actions it intended nationally and internationally for the 2020–2023 quadrennium.

The Strategy failed to materialize as originally planned in 2018. In particular, E-Ciber left the purview of the National Information Security Policy and became linked to PNCiber, established in 2023, together with the National Cybersecurity Committee, via Decree no. 11,856 (Brasil, 2023). The National Cybersecurity Committee is a collegiate linked to the Institutional Security Office of the Presidency of the Republic. Decree no. 11,856 provided that E-Ciber should be updated in the following years, extending the validity of the previous version until its replacement. The new E-Ciber was published in August 2025 (Brasil, 2025).

PNCiber Art. 3, establishes 11 objectives; four of which are affected by CYBEROS to a greater or lesser extent: I) to develop national products, services, and technologies aimed at cybersecurity; VII) to offer education and technical-professional training in cybersecurity in society; VIII) to foster cybersecurity scientific research, technological development, and innovation activities; and IX) to increase the coordinated action and exchange of cybersecurity information between the Union, the states, the Federal District and the Municipalities, the Executive, Legislative, and Judicial Branches, the private sector, and society in general.

E-Ciber must achieve the PNCiber objectives. It is structured in four thematic axes: I) protection and awareness of citizens and society, II) security and resilience of essential services and CIs, III) cooperation and integration between public and private bodies and entities, and IV) national sovereignty and governance. Specific strategic actions provided for in the National Cybersecurity Plan (which is still to be developed) must implement these thematic axes. In this sense, the current E-Ciber differs structurally from the previous 2020 one, replacing its strategic objectives with thematic axes and leaving the definitive mapping of strategic actions to the National Plan. In any case, the current E-Ciber has a list of minimum actions for each of its axis.

Regarding the 14 actions related to thematic axis I, four are related to a greater or lesser degree with CYBEROS: IV – incentive to the training of public and private teachers and managers in cybersecurity; V – encouragement of the inclusion of topics related to cybersecurity in all educational curricula; VI – stimulus toward participation in academic, technical, and professional forums and activities related to cybersecurity; and IX – motivation to develop institutional contingency plans and to carry out tests and simulations to assess the level of cybersecurity in agencies or entities. The context of the development of CYBEROS at IME (a higher education institution) and its insertion in LaSC (as discussed in section 2) justify its alignment with actions IV, V, and VI. Action IX is partially met regarding the issue of tests and simulations since CYBEROS and its verticals propose to serve as a tool to simulate various cybersecurity scenarios, especially in CI protection.

Thematic axis II, which refers to essential services and CIs, specifies a minimum of 11 actions to achieve its related objectives. Interestingly, despite the prominence of CYBEROS regarding CI protection scenarios, only one action can be highlighted as directly related: VIII – encouragement of regular sectoral and multisectoral exercises and simulations to improve the resilience of essential services and CIs. CYBEROS is a tool that will be available for IME, academia,

and the productive sector for exercises and simulations of interest to the institutions responsible for national CIs.

Thematic axis III also only lists a single action (of a total of five) to which CYBEROS and the context in which it fits can contribute. Its Action I aims to encourage the creation and development of cybersecurity incident prevention and response teams, information analysis and sharing centers, and specialized cybersecurity laboratories. LaSC, the laboratory that developed and hosts CYBEROS, certainly fits the role of a laboratory specialized in cybersecurity and, as such, able to develop teams to address cyber incidents.

Finally, axis IV lists 10 minimum actions to meet and protect the interests of Brazilian society in cyberspace and ensure a reliable cyber environment that guarantees its economic and technological growth. Half of these actions are in line with the potential of CYBEROS, whereas two others align themselves with the academic context in which CYBEROS fits: III – technical-professional training in cybersecurity on a scale compatible with national needs and IX – incentive to the creation of lines of research for *stricto sensu* undergraduate and graduate studies and the granting of scholarships to train Brazilian specialists and teachers in cybersecurity. Also, two other actions refer to the innovative potential of the tool, the participation of a strategic defense company in its development and the promotion by public resources mainly obtained via Funding Authority for Studies and Projects: IV – reduction of the Brazilian technological debt in emerging and disruptive technologies via affirmative and incremental government actions and X – incentive to the development of national products, services, and technologies to improve cybersecurity in the country. CYBEROS can also contribute to action V – incentive to the development of capacity of continuously assessing conformity in cybersecurity product, service, and technology security (discussed regarding the CYBEROS tactical radio network vertical in section 5).

4.3 PNSIC/ENSIC

The attention of the Brazilian State to CI security grew at the end of the 2000s, evidenced by the inclusion of this concern in the first version of the NDS in 2008. The discussions since then led to the approval of the PNSIC (Brasil, 2018a), and afterwards the publication of Decree no. 9819, in 2019, inserting CI protection in the list of competencies of the Chamber of Foreign Affairs and National Defense of the Council of Government.

The PNSIC defines CIs as facilities, services, goods, and systems whose total or partial interruption or destruction would cause serious social, environmental, economic, political, international, or security impact on the state and society. It also characterizes CI security as a set of preventive and reactive measures to preserve or reestablish CI-related services. It also provides guidelines for joint efforts to be developed by public and private sector bodies and entities regarding this.

The Decree that established the PNSIC defined the need to establish the ENSIC as an instrument for its implementation. ENSIC, published in 2020 (Brasil, 2020b), consolidates the concepts and lists the main challenges for the CI security activity. It established four structuring axes (SA) constituting the main pillars for CI security effectiveness. The axes organize the

challenges aiming to create an organically coherent and cohesive strategy that should boost CI security. ENSIC establishes strategic objectives for each SA, arranging them under no specific priority, describing the strategic focus in direct efforts to implement the PNSIC and signaling the desired results. Several tactical initiatives use strategic objectives, guiding the effective use of these efforts.

CYBEROS contributes to two SA from ENSIC. Its first alignment is with SA 2 – Awareness and training, in its strategic objective 2.2 (foster training and education in CI security) and, more specifically, strategic initiative 2.2.1 (foster training actions in CI defense and security). The creation of LaSC took place precisely in the context of state concerns with CI security, and the development of CYBEROS, especially considering its customization for this scenario, reinforces such alignment.

The other contribution to ENSIC regards SA 4 (data and information management) and its strategic objective 4.3 (Encourage the adoption of resources and procedures aimed at cybersecurity in CIs) and strategic initiative 4.3.2 (Guide CIs to observe E-Ciber), especially the provisions of item 2.3.5 (Raise the protection level of national CIs). The CYBEROS contribution to the trio between structuring axes and strategic objectives and initiatives is evident since the system is a tool to support realistic cyber studies and training that supports the generation of specialized knowledge to prepare specific procedures and action plans to be adopted by institutions and personnel in CI security.

5 CONTRIBUTIONS FROM THE TACTICAL RADIO NETWORKS VERTICAL

One of the main innovations of CYBEROS lies in its tactical radio network vertical. It incorporates a radio frequency channel emulator that can controllingly degrade signals, simulating complex field environments within a controlled laboratory in automated tests with physical or virtualized SDR modules. The realistic simulations of the vertical can execute performance, interoperability, and resilience tests under conditions equivalent to those of real civil or military operations. It also enables comprehensive vulnerability analyses, mapping critical threats to SDR-based networks in a structured way. It contributes to standardization and certification since test results help the development and use of a normative basis for cybersecurity. It expands the list of models for experiments in hybrid scenarios that combine attacks on the electromagnetic spectrum and cyber threats. Finally, it provides technical support for timely meeting security and performance demands, helping to preserve informational superiority and command and control capacity in highly contested scenarios.

The tactical radio network vertical streamlines the identification of new threats and the execution of countermeasure tests for systems that support CI, implementing functionalities to simulate and analyze vulnerabilities. This is vital for improving security devices and adopting alternative protection procedures since cyber threats evolve at a rapid pace. Task automation also optimizes efforts, reducing costs and incident response time. As private companies operate a large portion of CIs, the tactical radio network vertical can also provide collaboration and the

sharing of standardized information between the public and private sectors, promoting a more integrated and effective governance of cybersecurity (Cravo, 2023; Gomes; Laginestra, 2023; Reis, 2024).

The agile and automated experimentation from the vertical accelerates the RD&I of new communication and electronic warfare capabilities, keeping Brazil ahead of potential adversaries. A country with advanced cyber capabilities and a robust defense strategy gains international respect and prominence, strengthening its diplomatic and cooperation position (Cravo, 2023).

As stated in subsection 4.1, CYBEROS verticals contribute to the development of cyber capability in the industry and military fields. The radio network vertical provides proactive identification and mitigates software and protocol vulnerabilities, which are fundamental to improve network and system security. Simulations of electromagnetic spectrum attacks and cyber threats can find vulnerabilities before they become real incidents, minimizing possibly catastrophic losses. This includes denial-of-service attacks (one of the biggest threats against Brazil) by simulating radio jamming or the disruption of essential services. This radio network vertical can perform waveform tests in virtualized and physical SDR, which enables the AF and the productive sector to evaluate the effectiveness and security of new communication technologies before their implementation, accelerating the development of national solutions and helping to reduce external technological dependence. The use of this vertical can also increase the frequency and realism of exercises such as Cyber Guardian Exercise, continuously and efficiently testing the resilience of tactical communication systems (Cravo, 2023; Gomes; Laginestra, 2023).

By facilitating simulations of complex scenarios and attack response, the vertical constitutes a powerful tool to empower and train the scarce human resources of the AF and other sectors of society in cybersecurity (Fontes, 2024; Cravo, 2023). The vertical can also enhance strategic intelligence, generating useful knowledge on trends and scenarios of highly complex cyber threats for technicians and managers in cyber defense (Melo; Albuquerque; Mendonça, 2022).

Another contribution of the radio network vertical is as an experimentation and certification tool that can more cohesively converge efforts between societal actors and facilitate the implementation of cybersecurity policies, guidelines, regulations, and specific requirements (Cravo, 2023; Gomes; Laginestra, 2023).

6 FINAL CONSIDERATIONS

This study reflected on the contributions of CYBEROS—a cyber range customized for cyber exercises with realistic scenarios of CI protection and uses military tactical radio

networks—to national defense. The context in which this system was developed was relevant in this discussion due to several aspects highlighted throughout this text.

This study described CYBEROS and its environment to highlight its most relevant characteristics with a potential connection with national defense demands. A more objective alignment required a qualitative research on high-level normative national defense documents that were pertinent to the main themes contextualizing the system: cyber security and IC protection. Thus, we identified and analyzed three pairs of national policies and strategies: NDP/NDS, PNCiber/E-Ciber, and PNSIC/ENSIC. The analysis of the specific potential contributions of the tactical radio network vertical linked to CYBEROS also considered other relevant tactical or operational references in a complementary way.

The system in this study contributes to the addressal of several of the main challenges in defense science, technology, and innovation, especially in strategic cybertechnology, such as dependence on foreign technologies, technological denial and the need for training human resources. It clearly pointed out how the system contributes (or can contribute) to objectives, strategies, and strategic actions of the three most relevant pairs of high-level national defense documents. It also discussed several complementary reflections regarding the specific potential of the chosen tactical radio network vertical to contribute to national defense. In short, CYBEROS and its verticals are a tool that helps Brazil to strengthen its technological sovereignty and position itself as a relevant actor in international cybersecurity defense.

ACKNOWLEDGMENTS

This study belongs to the ITSC2ICCOM project. It received financial support from the Funding Authority for Studies and Projects (FINEP) — Contractual Instrument, Code no. 01.22.0523.00 (Ref. 1890/22). We would also like to thank the LaSC members who directly or indirectly contributed to the feasibility of this study.

REFERENCES

ADIWAL, Sanjay; MISBAHUDDIN, Mohammad. Intrusion Detection and Prevention in OpenStack: A Case Study on Enhancing Security and Threat Detection. **SN Computer Science**, v. 4, n. 830, 2023. DOI: 10.1007/s42979-023-02265-3

AL-SHARA, A.; AHMAD, M. **Cyber Warfare**: Attacks and Countermeasures. Cham: Springer, 2018.

BAGGA, J. Introduction to APIs. *In*: BAGGA, J. **Introduction to Integration Suite Capabilities**. Berkeley: Springer, 2023.

BALDINI, G. *et al*. Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead. **IEEE Communications Surveys & Tutorials**, v. 14, n. 2, p. 355-379, 2012. DOI: 10.1109/SURV.2011.032511.00097

BARBOSA, F. G. F. T.; CALDEIRA, A. B. Desafios da inovação como estratégia para a geração de capacidades militares terrestres. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 15, n. 54, p. 273-293, 2021.

BARROS, M. Instituto Militar de Engenharia Capacita Militares para Cyber Flag 24-1. **Defesa em Foco**, 17 jun. 2024. Available at: https://www.defesaemfoco.com.br/instituto-militar-de-engenharia-capacita-militares-para-cyber-flag-24-1/. Access on: Aug. 6, 2025.

BARROS, M. Cyber Shield 2025: Defesa Cibernética do Brasil em destaque nos EUA. **Defesa em Foco**, 10 jun. 2025. Available at: https://www.defesaemfoco.com.br/cyber-shield-2025-defesa-cibernetica-do-brasil-em-destaque-nos-eua/. Access on: June 25, 2025.

BERGSTROM, C. *et al*. Software defined radio (SDR) special military applications. **MILCOM 2002**, Anaheim, v. 1, p. 383-388, 2002. DOI: 10.1109/MILCOM.2002.1180472

BRANCO, M. G. C. *et al*. Rádio Definido por Software do Ministério da Defesa – Visão geral das primeiras contribuições do CPqD. **Cadernos CPqD Tecnologia**, v. 10, n. esp., p. 9-16, 2014.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, DF, 2008.

BRASIL. Presidência da República. Decreto nº 9.573, de 22 novembro de 2018. **Diário Oficial da União**, Brasília, DF, 2018a.

BRASIL. Presidência da República. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997. **Diário Oficial da União**, Brasília, DF, 2018b.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia Nacional de Segurança Cibernética**. Brasília, DF, 2020a.

BRASIL. Presidência da República. Decreto nº 10.569, de 9 dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial da União**, Brasília, DF, 2020b.

BRASIL. Presidência da República. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. **Diário Oficial da União**, Brasília, DF, 2023.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Decreto Legislativo nº 61, 23 mai. 2024. Brasília, DF, 2024a.

BRASIL. Exército Brasileiro. Exército coordena o maior exercício cibernético do Hemisfério Sul. **Noticiário do Exército**, Oct. 11, 2024b. Available at: https://www.eb.mil.br/web/noticias/w/exercito-coordena-maior-exercicio-cibernetico-do-hemisferio-sul. Access on: Aug. 6, 2025.

BRASIL. Presidência da República. **Decreto nº 12.573, de 4 de agosto de 2025**. Institui a Estratégia Nacional de Cibersegurança. **Diário Oficial da União**, Brasília, DF, 2025.

CAMARGO, O. A. M. *et al*. Laboratório de Segurança Cibernética para Análise de Malwares Reais em Infraestruturas Críticas. **Congresso Brasileiro de Automática - CBA**, v. 3, n. 1, 2022.

CASTILHO, C. A. C. **A Segurança Cibernética na proteção das infraestruturas críticas brasileiras**. Trabalho de Conclusão de Curso (Curso Superior de Segurança e Defesa Cibernética) – Escola Superior de Guerra, Rio de Janeiro, 2023.

CONTI, M. *et al*. Internet of Things security and Forensics: Challenges and Opportunities. **Future Generation Computer Systems**, v. 78, p. 544-546, 2018. DOI: 10.1016/j.future.2017.07.060

CRAVO, C. V. **Em busca de uma estratégia nacional de segurança cibernética: marco legal e autoridade nacional de segurança cibernética**. 2023. Tese (Doutorado em Estudos Estratégicos Internacionais) – Programa de Pós-Graduação em Estudos Estratégicos Internacionais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023. Available at: https://lume.ufrgs.br/handle/10183/263232. Access on: Aug., 6, 2025.

FELLER, J. *et al*. (orgs.). **Perspectives on Free and Open Source Software**. Cambridge: MIT Press, 2005.

FONTES, P. R. **A contribuição da Inteligência Estratégica para a Defesa Nacional contra Ameaças Cibernéticas**. 2024. Trabalho de Conclusão de Curso (Especialização em Inteligência Estratégica) – Escola Superior de Defesa, Brasília, DF, 2024.

FUNDAÇÃO DE APOIO À PESQUISA, DESENVOLVIMENTO E INOVAÇÃO DO EXÉRCITO BRASILEIRO – FAPEB**. ITS2ICCOM – Convênio FINEP-FAPEB Nº 01.22.0523.00**. Rio de Janeiro: FAPEB, 2022. Available at: https://fapeb.com.br/its2iccom-convenio-finep-fapeb-no-01-22-0523-00/. Access on: Aug., 6, 2025.

FUNDAÇÃO DE APOIO À PESQUISA, DESENVOLVIMENTO E INOVAÇÃO DO EXÉRCITO BRASILEIRO – FAPEB. **Chamada Pública nº 05/2025 – ITS2ICCOM**: contratação de serviço de desenvolvimento e entrega de um orquestrador e provisionador de ambientes virtualizados heterogêneos completos. Rio de Janeiro: FAPEB, 2025. Available at: https://fapeb.com.br/wp-content/uploads/2025/06/EDITAL-PARA-CHAMADA-PUBLICA-PROJETO-ORQUESTRADOR-ERRATA-DE-CRONOGRAMA.pdf. Access on: Aug., 6, 2025.

GOMES, N. L. S.; LAGINESTRA, A. M. Governança da Segurança Cibernética e os desafios do século XXI: a relação civis-militares no sector cibernético do Brasil. **Revista Foco**, Curitiba, v. 16, n. 7, p. 1-17, 2023. DOI: 10.54751/revistafoco.v16n7-056

HEINÄARO, K. Cyber attacking tactical radio networks. *In*: **International Conference on Military Communications and Information Systems (ICMCIS)**. Cracóvia, 2015. p. 1-6. DOI: 10.1109/ICMCIS.2015.7158684

INSTITUTO MILITAR DE ENGENHARIA – IME. **Pós-Graduação em Proteção de Sistemas Elétricos (PGPSE)**. Rio de Janeiro, 2025. Available at: https://pgpse.ime.eb.br/. Access on: Aug., 6, 2025.

KLOTH, S. *et al*. Towards a Cyber Defense System in Software-Defined Tactical Networks. *In*: **International Conference on Military Communication and Information Systems (ICMCIS)**, 2024. p. 1-8. DOI: 10.1109/ICMCIS61231.2024.10540952

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de Metodologia Científica**. 8. ed. São Paulo: Atlas, 2017.

LI, K. *et al*. Security Mechanisms to Defend against New Attacks on Software-Defined Radio. In: **International Conference on Computing, Networking and Communications (ICNC)**, Maui, p. 537-541, 2018. DOI: 10.1109/ICCNC.2018.8390381

LILLEMETS, P. *et al*. A Systematic Review of Cyber Range Taxonomies: Trends, Gaps, and a Proposed Taxonomy. **Future Internet**, v. 17, n. 6, p. 259, 2025. DOI: 10.3390/fi17060259

MALAGUTTI, M. Ameaças ao Ciberespaço, Logística e Segurança Nacional, Não Necessariamente nessa Ordem. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 16, n. 57, p. 417-441, 2022.

MEDEIROS, B. P.; CARVALHO, A. C.; GOLDONI, L. R. F. Uma análise sobre o processo de securitização do ciberespaço. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 13, n. 46, p. 45-66, 2019.

MELO, R. C. R.; ALBUQUERQUE, R. O.; MENDONÇA, F. L. L. Modelo para mapeamento de ameaças cibernéticas. *In*: Iberian Conference on Information Systems and Technologies (CISTI), 17., 2022. **Anais** [...]. Madrid, 2022. p. 1-745.

MOREIRA, R. G.; GALDINO, J. F. A "dualidade" da dualidade tecnológica: implicações para países em desenvolvimento. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 18, n. 62, p. 189-216, 2024.

OKABAYASHI, V. H. **Defesa cibernética em infraestruturas críticas: estratégias avançadas para mitigação de ameaças**. 2024. Trabalho de Conclusão de Curso (Curso de Altos Estudos de Política e Estratégia) — Escola Superior de Guerra, Rio de Janeiro, 2024.

OR-MEIR, O. *et al*. Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. **ACM Computing Surveys**, v. 2, n. 5, 2019. DOI: 10.1145/3329786

PINHEIRO, A. S. A tecnologia da informação e a ameaça cibernética na guerra irregular do século XXI. **Coleção Meira Mattos**, Rio de Janeiro, n. 18, p. 4-11, 2008.

REDAÇÃO TECNOLOGIA & DEFESA. RDS-RONDON, mais um integrante da família RDS-DEFESA. **Tecnologia & Defesa**, 5 fev. 2024. Available at: https://tecnodefesa.com.br/rds-rondon-mais-um-integrante-da-familia-rds-defesa/. Access on: Aug, 6, 2025.

REIS, J. P. **Segurança cibernética: uma abordagem conceitual com elementos de análise de risco**. 2024. Trabalho de Conclusão de Curso (Especialização em Inteligência Estratégica) – Escola Superior de Defesa, Brasília, DF, 2024.

SANDOVAL, A. A. J. Como a tecnologia está controlando nossa infraestrutura crítica, civis e militares trabalhando juntos para minimizar ciberataques. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 14, n. especial, p. 153-168, 2020.

SANTOS JUNIOR, J. B. S. *et al*. Novas ameaças e a cibersegurança: uma análise do sistema brasileiro de defesa cibernética frente ao caso da espionagem durante o governo Dilma Roussef. *In*: **Congresso Acadêmico de Defesa Nacional**, 2019, Rio de Janeiro, v. 1, p. 110-120. Available at: https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/xvi_cadn/novasa_ameacasa_ea_aa_ciberseguranca_umaa_analisea_doa_sistemaa_brasileiroa_dea_defesaa_cibernetica.pdf. Access on: Aug., 6, 2025.

SCHWETHER, N. A evolução e o futuro da Ciberguerra: um estudo aprofundado de Portugal. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 18, n. 63, p. 463-479, 2025.

SILVA, F. A. B.; MOURA, D. F. C.; GALDINO, J. F. Classes of attacks for tactical software defined radios. **International Journal of Embedded and Real-Time Communication Systems**, v. 3, n. 4, p. 57-82, 2012. DOI: 10.4018/jertcs.2012100104

SILVA, F. A. B.; MOURA, D. F. C.; GALDINO, J. F. Security Issues in Tactical Software-Defined Radios: Analysis of Attacks and Case Studies. *In*: **ADVANCING EMBEDDED SYSTEMS AND REAL-TIME COMMUNICATIONS WITH EMERGING TECHNOLOGIES**. Hershey: IGI Global, 2014, p. 22-53.

SNEPS-SNEPPE, M. On Cyber Threats in Military Communication Nets. *In*: **IEEE WORKSHOP ON MICROWAVE THEORY AND TECHNOLOGY IN WIRELESS COMMUNICATIONS (MTTW)**, Riga, Latvia, 2024. p. 12-17. DOI: 10.1109/MTTW64344.2024.10742192

SOUZA, R. C. S.; OLIVEIRA, T. F. D.; PAULA, M. G. A Guerra Cibernética Russo-Ucraniana: os ataques russos às Infraestruturas Críticas ucranianas e possíveis lições para o Exército Brasileiro. **Coleção Meira Mattos: Revista das Ciências Militares**, Rio de Janeiro, v. 18, n. 61, p. 143-158, 2024.

ŠVÁBENSKÝ, V. *et al*. Cybersecurity knowledge and skills taught in capture the flag challenges. **Computers & Security**, v. 102, p. 102154, 2021. DOI: 10.1016/j.cose.2020.102154

TANG, C. Meta's Hyperscale Infrastructure: Overview and Insights. **Communications of the ACM**, v. 8, n. 1, 2025. DOI: 10.1145/3629263

THOMAS, J.; FIALA, M. Resilient Tactical Communications in Adversarial Environments. **Defence Technology Review**, v. 28, 2020.

VU, L. *et al*. A Cyber-HIL for Investigating Control Systems in Ship Cyber Physical Systems Under Communication Issues and Cyber Attacks. **IEEE Transactions on Industry Applications**, v. 60, n. 2, p. 2142-2152, 2024. DOI: 10.1109/TIA.2023.3311429