ARTICLE DOI 10. 52781/cmm.145

The evolution and Future of Cyberwar: an in-depth study of Portugal

La evolución y el futuro de la ciberguerra: un estudio en profundidad de Portugal

Abstract: This article analyzes the war of the future from the lens of cybernetics analysis. The aim is to answer the general question: how has Portugal organized itself to fight future warfare? And, more specifically: what is the role of cybernetics in the country's preparation? For this purpose, we opted to perform the exploration and global analysis of strategic documents from the government and the Portuguese Armed Forces, which allow us to further understand the dynamics of the case. The study reveals the prioritization and attention recently conquered by the fields of cyber domain within the country, with significant actions such as the creation of the Cyberdefense Operations Command.

Keywords: Strategy; Planning; Cybernetics; Case Study; Portugal.

Resumen: Este artículo analiza la guerra del futuro desde un análisis cibernético. El propósito es responder al interrogante central: ¿Cómo viene organizándose Portugal para luchar en la guerra del futuro? Y, más concretamente, ¿cuál es el papel de la cibernética en la preparación de este país? Para ello, se adopta la exploración y análisis de documentos estratégicos del Gobierno portugués y de las Fuerzas Armadas portuguesas para comprender con mayor profundidad la dinámica del caso. Este estudio reveló la reciente priorización y la atención prestada al ámbito cibernético en el país, con acciones significativas como la creación del Comando de Operaciones de Ciberdefensa.

Palabras clave: Estrategia; Planificación; Cibernética; Caso de estudio; Portugal.

Natália Diniz Schwether
Universidade Federal de Santa Catarina
Florianópolis, SC, Brasil.
E-mail: n.schwether@unesp.br

Received: June 7, 2023
Accepted: Sept. 27, 2024

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

* This study was carried out with the support of the Brazilian Federal Agency for Support and Evaluation of Graduate Education (CAPES) – Financing Code 001

1 INTRODUCTION

In the last decade, the use of cyberspace for strategic planning of states and their armed forces progressively gained relevance. Within the North Atlantic Treaty Organization (NATO) framework, the heads of the member states announced, in 2014, cyber defense as one of the group's objectives and observed the need to improve capacities in this area (NATO, 2014).

A few years later, in 2016, they formally recognized cyberspace as the fourth domain of military operations. More recently, in 2022, NATO's Strategic Concept reaffirmed that safe and unrestricted access to cyberspace are fundamental for a collective dissuasion and defense (NATO, 2022).

Cyber defense is also a priority in the European Union (EU). In 2020, the EU Cybersecurity Strategy declared cyberspace as a military domain, and in 2022, the Strategic Compass for Security and Defence signed a commitment to develop a policy for this sector.

Portugal, a southern European state, member of the European Economic Community since 1986 and a founding member of NATO, has also been developing initiatives ensuring free and safe use of cyberspace (Pinho, 2020).

Among them, the following stand out: the Strategic Concept of National Defense (2013), which pointed cybercrime as one of the main risks to national security, definition of the *Orientação Política para a Ciberdefesa* (Political Orientation for Cyber Defense) (2013), creation of the Cyber Defense Center (CDC) of the Armed Forces (2014) and the *Centro Nacional de Cibersegurança* (CNCS –Portuguese National Cybersecurity Center, 2014), the *Estratégia Nacional de Cibersegurança* (National Strategy for Cyberspace Security, 2015 and 2019) and the *Estratégia Nacional de Ciberdefesa* (National Cyber Defense Strategy, 2022).

Given this context, the Ministry of National Defense considered cyber defense a priority, stating that it is imperative to qualify human resources assigned to the area (Order No. 10309/2022).

Hence, this article aims to answer the question: how has Portugal organized itself to fight future warfare? And specifically: what is the role of cybernetics in the country's preparation? Considering the constant and unpredictable evolution of war, which develops in parallel to battlefield expansion, covering a variety of domains and means (cybernetic, spatial, cognitive, and informational) to be possibly used by adversaries in the future operational environment (Schwether, 2021).

Therefore, the exploratory research method will be used, which, by describing Portugal's main strategic documents of the last decade, allows us to understand the defense planning stages and how the cyber sector evolved and organized itself.

The description is necessary to answer questions such as "when," "who," and "which." The inferential quality of a description is directly associated with quality of data sources, measurement instruments or coding procedures (Gerring, 2012).

That being said, this introduction is followed by three sections. The first addresses what we call a grand strategy, that is, a plan with a holistic and multidimensional view of a state's action

priorities (Reis, 2019). The second section focuses on the Portuguese Armed Forces' strategic planning system, compiling the documents that guide the construction of future capabilities. In the third section, we narrow the scope of analysis to cyber capability and its evolution at strategic and organizational levels. Finally, the conclusion ponders important advances achieved and obstacles still to be faced.

2 GRAND STRATEGY

The strategic transatlantic link between the United States, Canada, and Europe was institutionalized by the North Atlantic Treaty in 1949. Since then, this relationship is fundamental to define Europe's defense and security strategies and policies, as well as to affirm Portugal's foreign policy.

One of the key documents formulated by NATO, presenting a strategic plan for the future, is the Strategic Concept. Since 1991, this document publicly describes the Alliance's priorities and provided important guidance to member states' military institutions. The importance of Portugal's national interests being reflected in the agreed great common principles and national planning are observed in this publication (Reis, 2022; Serronha, 2010).

The Strategic Concept approved in Lisbon, at the end of 2010, focused on three issues: collective defense, crisis management, and cooperative security. One of the most important features is the organization's scope of action, that is, if a member is at risk, the Alliance can act outside its own borders. It also plans to be actively involved in international security by proposing partnerships with other countries and organizations (Fernandes, 2013).

However, Portugal's foreign policy failed to incorporate several issues sought by the country's diplomacy, especially regarding expansion of partnerships towards the South Atlantic (Fernandes, 2013). Portugal's maritime vocation is crucial to its international assertiveness, and the Atlantic is an area of strategic interest.

Ten years after the approval of the last Strategic Concept, and with the increasing digitalization of society and complexity of global security and defense, another formal process to review the document began.

The Madrid Strategic Concept, approved in 2022, while reaffirming the organization's principles[1], also presented a new list of potential adversaries, including China and Russia. It also highlighted emerging new technologies and growing interest in space and cybernetic domains (Daehnhardt; Gaspar, 2020; Gaspar, 2022; Garcia, 2022; Daehnhardt, 2022).

The Strategic Concept is one of the central inputs to formulate the *Conceito Estratégio de Defesa Nacional* (CEDN – Strategic Concept of National Defense) in Portugal. The CEDN is the main instrument to present the national strategy for defense and security and a tool to coordinate efforts of various state agencies in mitigating national concerns[2] (Portugal, 2013a).

1 Collective defense and deterrence are the main principles.

2 They are: terrorism, proliferation of weapons of mass destruction, transnational organized crime, cybercrime, and piracy.

The document, approved in 2013, recommends for the Armed Forces to act together in all spheres, from concepts, doctrines, and procedures to institutional and organizational culture. It also proposes reorganizing and simplifying structures, aiming for greater efficiency, agility, modularity, and flexibility. Strategically, the CEDN determined that investments should be oriented according to required capacities to fulfill priority missions (Portugal, 2013a).

Regarding cyber environment, some objectives were outlined, including definition of a National Cybersecurity Strategy, establishment of technical bodies, user awareness and improvement of national cyber defense capacity. To this end, better strategic communication by the Armed Forces and promotion of research and innovation are essential (Portugal, 2013a).

After all, although the technological component is often an important initial condition for innovations, a true military revolution depends on the confluence between weapons, operations, organization, and vision of future warfare (Adamsky, 2010). The state's role is just as important, as a driving agent capable of investing in research, defining priority areas and formulating long-term strategies (Storti; Ferreira, 2022).

In other words, as the future of war places more demands and moves limited resources of states in opposite directions, they are responsible for making great strategic choices (Cohen et al., 2020).

Whether due to the pandemic's repercussions or the end of peace in Europe in 2022, it became crucial to review the CEDN, encouraged by initiatives promoting public debates on topics of interest and by personalities of recognized merit, who met to reflect on the issues (Conselho, 2023).

In 2023, the *Relatório de Revisão do Conceito Estratégico de Defesa Nacional* (Review Report of the Strategic Concept of National Defense) was presented. The proposal, approved in May, is an integral element of the CEDN review process and will be part of the final version, set to be passed by the Council of Ministers, Prime Minister and Minister of National Defense.

In the document, the dispute for cyberspace dominance and expansion of cyber capabilities of state and non-state actors were pointed out as challenges to strategic stability and security. As well as competition in cyberspace and sophistication of attacks and damage they can inflict, especially on critical infrastructure, it was considered one of the biggest threats, difficult to anticipate and likely to affect basic social functions and citizens' well-being (Conselho, 2023).

It also stated the need to improve the country's defense and resilience capabilities, in addition to establishing cooperation in the defense field, increasing the capacity of the military industry and strengthening the Armed Forces' capabilities, ensuring necessary structures and mechanisms for integrated action in different operational areas (Conselho, 2023).

Specifically, it recommended developing national capacity in space and cyberspace and planning acquisition of new means, equipment, and systems to build full spectrum of military capabilities in the medium and long-term, in parallel with the valorization and qualification of

the Forces' human dimension, deepening the professionalization process of the military system (Conselho, 2023).

Finally, the analysts suggested shorter time frames for reviewing and implementing mechanisms to monitor actions, such as changing the document's name from *Conceito Estratégico de Defesa Nacional* (Strategic Concept of National Defense) to *Estratégia de Segurança e Defesa* (Security and Defense Strategy). In the future, the document may be the basis for a National Security Strategy (Conselho, 2023)[3].

3 STRATEGIC PLANNING IN DEFENSE

Portugal has a strategic planning system that, essentially, remained unchanged for about four decades. Established in the 1980s, it was designed to be developed sequentially and hierarchically, starting with the CEDN (discussed in the previous section), followed by the *Conceito Estratégico Militar* (CEM – Strategic Military Concept), the definition of the *Missões das Forças Armadas* (MIFA – Armed Forces Missions), the *Sistema de Forças Nacional* (SF – National Force System), and the *Dispositivo de Forças* (Force Device) (Rodrigues, 2020).

Figure 1. Strategic Planning in Defense

Source: Prepared by the author, 2023.

The CEM, among others, identifies strategic military objectives, modalities of military action to achieve these objectives and provides recommendations in terms of means. It is the responsibility of the Ministry of National Defense, proposed by the *Conselho de Chefes de Estado-Maior* (Chiefs of Staff Council) (Rodrigues, 2020).

The document, approved in 2014, is, until its revision, the main national instrument guiding construction of future capabilities, according to usage scenarios, military objectives and

3 The proposal aligns with the perception of Rodrigues (2020). The author claims that Portugal's CEDN is a strategy and not a concept and, therefore, must ensure harmony between objectives and means. An operational concept is essentially formulation of an idea as to how something can be done or accomplished and which may, therefore, lead to a certain procedure or capability. The concepts usually constitute a vision of how the Armed Forces intend to operate in the medium and long-term, based on changes observed in the scenario or in strategic domains. Concepts usually contain elements resulting from the combination of informed evaluation and innovative thinking (Nunes, 2016).

levels of ambition defined in it. Specifically on cyberattack cases, it instructs the Armed Forces will be called upon to:

> [...] ensure safeguarding of their information and protection of their communications infrastructures and information systems, supporting protection and defense of national critical infrastructures, as well as collaborate with other state institutions in the cybersecurity field, contributing to protection of populations and promoting their well-being (Portugal, 2023, our translation).

It also expresses concern to obtain diversified, interoperable and integrate capabilities, as well as intention to organize the Armed Forces focusing on modular, flexible, joint, and combined usage. Notably, however, the absence of a defined time frame makes the guidelines unlikely for the Armed Forces' long-term planning (Abreu, 2018; Pires, 2018).

The MIFAs aim to identify strategic-military level missions assigned to the Armed Forces and corresponding to concrete military tasks. The missions respect priorities and guidelines contained in the CEDN and the CEM.

Missions presented in the MIFAs, in 2014, focus on six areas: (a) security and defense of the national territory and citizens; (b) collective defense; (c) exercise of national sovereignty, jurisdiction, and responsibilities; (d) cooperative security; (e) support for development and well-being; and (f) military cooperation and assistance.

It is predicted, for national territory defense, the possibility to:

> [...] apply defensive and if necessary offensive measures against cyberattacks, to ensure safeguarding of information and protection of the infrastructures of Communications and Information Systems of the Armed Forces, as well as support in protection and defense of national critical infrastructures and the State's electronic government (Portugal, 2014, p. 3, emphasis added, our translation).

The SF identifies a set of capabilities that are required to fulfill the Armed Forces' missions, indicating types and quantities of forces and means, based on specific guidelines, usage scenarios, and operational complementarity.

The document, however, is not a reference for the development of programs and military reequipment, since it is restricted to being a list of units, infrastructures, agencies, etc., and does not present a vision for the future or anticipate modernization needs (Rodrigues, 2003).

In turn, the *Dispositivo de Forças* establishes the relationship between operational commands, Forces, units, and means with infrastructures that support them, materializing the way they organize and respond to various capabilities listed in the SF to fulfill the MIFAs.

Finally, the *Lei de Programação Militar* (LPM – Military Programming Law) is financially responsible for materializing military strategies capable of providing the Armed

Forces with necessary skills to fulfill their missions in terms of material (maintenance, replacement, or innovation) (Abreu, 2018).

Cyber defense is one of the projects included in the LPM, specifically those toward protection and security of critical infrastructure computer networks and Command and Control systems and provision of offensive capacity to the Armed Forces to neutralize potential threats. Compared with the 2015 and 2019 LPMs, the sector shows a significant increase in investments and maintenance of resources for the 2023-2034 period[4].

Notably, the budget allocated to cyber defense was never executed at more than 50%[5], either due to the pandemic, shortage of specialized human resources or delay in processing cases (Marcelino, 2023).

Moreover, the 2014-2019 strategic planning cycle was guided by the *Reforma Defesa 2020* (Defense Reform), of April 2013, which considered establishing more modern, operational, sustainable, and efficient Armed Forces. The guidelines were divided into two pillars: (i) a new strategic planning cycle and (ii) reorganization of the macrostructure. In terms of structure, the joint, modular, and flexible nature was valued. Among the specific guidelines was the increase of cyber defense capacity (Portugal, 2013b).

More recently, the *Diretiva Ministerial de Planeamento de Defesa Militar* (Ministerial Directive on Military Defense Planning), 2019-2022, approved in 2020, continued reinforcing the Forces' joint command and the relevance of integrating, with maximum effectiveness, the land, naval, and air component, as well as capabilities to operate in cyberspace (Portugal, 2020).

The directive also highlighted the commitment toward thinking about national defense, more specifically, renewal of structure, doctrine, and means, in light of new challenges such as space and cyberspace, artificial intelligence, and disinformation. As well as to act on it considering of the increasing frequency and intensity of cyberattacks and the challenge of new actors, technologies, and domains (Portugal, 2020).

4 ACTIONS IN CYBERSPACE

The first initiative, at the strategic level, was in 2013, with the *Orientação Política para a Ciberdefesa* (Political Guidance for Cyber Defense), a directive that would provide a substrate for building capacity in the sector.

The document established three main objectives: (i) ensure protection, resilience, and security of networks against attacks; (ii) the country's freedom of action in cyberspace—to ensure and, when necessary, prevent or hinder hostile use against national interest; and (iii) contribute collaboratively in the national context (Portugal, 2013c).

To achieve these objectives, seven courses of action were defined: (1) establish a national cyber defense framework; (2) integrate cyberspace operations within the framework of military capabilities; (3) conduct the full spectrum of military operations

4 LPM 2015-2026: total resources for Cyber Defense: 14,000; LPM 2019-2030: total resources for Cyber Defense: 45,490; LPM 2023-2034: total resources for Cyber Defense: 43,469.

5 In 2020, it was only 48.9%; in 2021 it fell to 27% and in 2022 it stood at 30.7% (Marcelino, 2023).

in cyberspace; (4) strengthen information capacity in cyberspace; (5) develop an early warning and information sharing system at various decision-making levels; (6) promote a risk management culture by incorporating its requirements into the procurement and supply chain; and (7) centralize training in cyber defense and adapt the management of human resources to ensure their permanence in these activities (Portugal, 2013c).

The document also identified the need to establish partnerships between state and private institutions, national and international, as a way to promote technological development, research, and innovation (Portugal, 2013c).

In 2015, cyber defense had its contours better defined when the *Estratégia Nacional de Segurança do Ciberespaço* (ENSC – National Strategy for Cyberspace Security) was published. It aimed to improve security of networks and information systems and enable a free, safe, and efficient use of cyberspace (Portugal, 2015).

To this end, six intervention guidelines were defined, namely: Guideline 1: Cyberspace security framework; Guideline 2: Combating cybercrime; Guideline 3: Protection of cyberspace and infrastructure; Guideline 4: Education, awareness, and prevention; Guideline 5: Research and development; Guideline 6: Cooperation. The first guideline includes functions specifically attributed to national defense, which are:

> a) Implement the Political Orientation for Cyber Defense, approved by Order No. 13692/2013, of October 11, published in the Official Gazette No. 208, 2nd series, of October 28, building the national cyber defense structure;
>
> b) Establish and consolidate a command and control structure for national cyber defense [...];
>
> c) Implement, develop, and consolidate cyber defense capability, to ensure conduct of military operations in cyberspace, safeguarding the country's freedom of action in cyberspace and, when necessary and determined, proactive use of cyberspace to prevent or hinder its hostile use against national interest;
>
> d) To make cyber defense an area where it is necessary to promote synergies and enhance dual use of its capabilities, within the scope of military operations and national cybersecurity, developing and consolidating an information sharing system at various decision-making levels (Portugal, 2015, emphasis added, our translation).

Lastly, the document stressed the importance of carrying out a regular and periodic review, within a three year limit, as well as an annual review of strategic objectives and lines of action, considering the changing circumstances (Portugal, 2015).

In 2019, the second ENSC was approved in Portugal, based on three strategic objectives: maximizing resilience, promoting innovation, and generating and guaranteeing

resources, which were translated into six intervention guidelines, very similar to those of the previous version (Portugal, 2019).

Regarding cyber defense, the goal is to strengthen the Armed Forces' resilience, and all means should be used to respond to cyberattacks, including offensive capacity. At the same time, it was intended to maximize the security and defense of networks and information systems using defensive cyber defense capability (Portugal, 2019).

This strategy highlights the need to increase dual use of cyber defense capabilities, developing and consolidating an information sharing system at various decision-making levels. It further mentions participating in cybersecurity and cyber defense exercises, aiming international cooperation and Portugal's affirmation in the field (Portugal, 2019).

In the wake of the ENSC and in light of the urgent need to densify concepts at the strategic level and to properly articulate structures dedicated to cyberspace, the ENCD was published in November 2022 (Nunes, 2018).

The ENCD reaffirms cyberspace as a military domain , of defensive and offensive operations, the latter being exclusive to the Armed Forces, ensuring defense and national interests in response to threats originating from states or non-state entities and dependent on political authorization (Portugal, 2022a).

Moreover, it establishes that the development of cyber capability must be aligned with other documents guiding military defense; that is, cyberspace is an integral element of the planning process, which values a multi-domain logic and operational flexibility, and the Armed Forces must ensure all command and control capabilities relevant to this new domain (Portugal, 2022a).

Four strategic objectives were also defined: to consolidate cyber defense capacity; maximize resilience and cohesion of national action; promote research, development, and innovation; ensure qualified resources. And six guidelines for the action plan: Guideline 1: use cyberspace as a domain of operations; Guideline 2: strengthen national cyber defense capacity; Guideline 3: create the cyber defense school; Guideline 4: intensify national and international cooperation; Guideline 5: promote research, development and innovation in cyberspace, encouraging the development of dual-use solutions; Guideline 6: ensure necessary cyber defense capabilities in state of exception contexts (Portugal, 2022a).

Regarding capacity building, three lines of action are priorities: increasing qualified personnel, having a technologically advanced infrastructure, and ensuring technological independence—promoting, for example, Industry 4.0, specially regarding workforce recruitment, selection, retention, and training (Portugal, 2022a, Serra, 2019).

Additionally, it proposed building a training center within the Armed Forces and in collaboration with other national and international reference entities. It also considered active participation in crisis management mechanisms, exercises, and international bodies working on cyberspace security to be important (Portugal, 2022).

At the organizational level, in 2014, the Cyber Defense Center (CDC) of the Armed Forces was created. The conception of the CDC, to date, shows its alignment with the institution's strategic thinking. The CDC is part of the structure of the *Estado-Maior-General das Forças Armadas* (EMGFA) (General Staff of the Armed Forces), made up of military personnel from

the three branches. Its main mission is to ensure integrity, confidentiality and availability of information and national defense information systems (Portugal, n.d.).

More recently, the 2022 *Lei Orgânica do Estado-Maior-General das Forças Armadas* (Organic Law of the General Staff of the Armed Forces) changed the structure, until then intended for cyber defense. With its approval, the EMGFA had its mission expanded, including, in addition to use of the Armed Forces in missions and operational tasks, military defense strategy, military higher education, military health, military information and security, cyber defense, military aspects of the national defense space program and innovation and transformation in the Armed Forces (Portugal, 2022b).

The EMGFA's new tasks aim to guarantee the fundamental principle of command and coordination unity, as well as continue to adapt the Armed Forces so they can operate in the multi-domain and face transnational and hybrid threats (Portugal, 2022b).

Two structures were created in the cyber domain: the *Centro de Comunicações e Informação, Ciberespaço e Espaço* (CCICE – Center of Communications and Information, Cyberspace and Space)**,** under responsibility of the *Chefe do Estado Maior General das Forças Armadas* (CEMGFA – Chief of the General Staff of the Armed Forces) and the *Comando de Operações de Ciberdefesa* (COCiber – Cyber Defense Operations Command) (Portugal, 2022b).

The CCICE's mission is to enable joint command and control capacity of the Armed Forces, ensure the command of military operations in and through cyberspace by the CEMGFA and manage military aspects of the national defense space program (Portugal, 2022b).

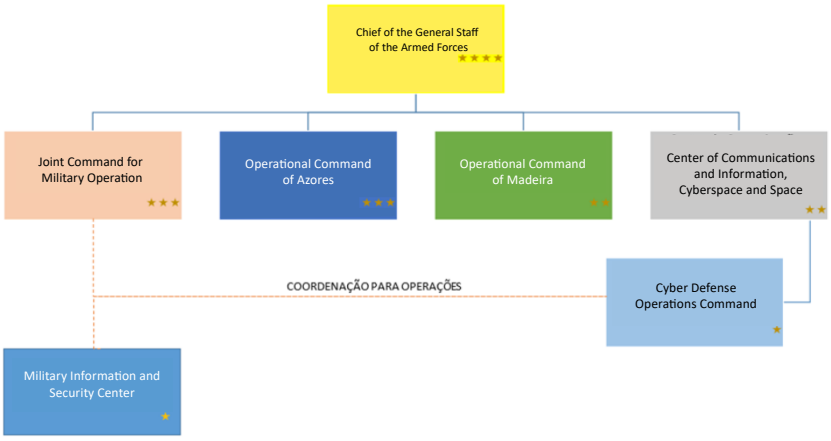
The CCICE is responsible for planning, coordinating, and implementing information and communications systems security and incident response measures for protection and resilience of the joint technological infrastructure, as well as proposing and conducting military operations in and via cyberspace in support of military objectives, participating in and organizing joint and combined cyber defense exercises, providing and coordinating the cyber defense capability, and acting in liaison and close cooperation with the national structures responsible for the security of cyberspace. The CCICE will encompass the *Escola de Ciberdefesa* (ECD – School of Cyber Defense) in its structure (Portugal, 2022b).

COCiber is responsible for planning, directing, controlling, and executing operations in and across cyberspace. Its structure can be reinforced by elements or units of the Forces' branches, as well as for development of operations and for planning and conducting of joint or combined exercises. It also relates to international structures linked to cyber defense and cyber security within NATO and the EU. Its structure also comprises the *Força de Operações de Ciberdefesa* (Cyber Defense Operations Force) (Portugal, 2022b).

In terms of cybersecurity, each Force is responsible for responding to incidents of its CIS, under the coordination of COCiber. In case of incidents the Force cannot resolve autonomously, COCiber takes tactical control, being responsible for responding to the incident (Pereira, R., 2022b).

COCiber aims to contribute for better operational articulation, enhancing coordination between the EMGFA and the Forces' branches and providing for a direct relationship with the *Comando Conjunto para as Operações Militares* (CCOM – Joint Command for Military Operations), bringing cyberspace closer to other domains of warfare (Pereira, B., 2022).

Figure 2. Defense Organizational Chart



Source: Bruno Pereira (2022).

Thus, with the restructuring of the cyber capacity, cyber defense components of each Force came under the COCiber's sphere, enabling greater interoperability and giving the Command a central role in national cyber defense (Nunes, 2020).

Regarding the material angle, the *Plano de Desenvolvimento da Capacidade de Ciberdefesa* (PDCCD – Cyber Defense Capability Development Plan) 2021-2021, states the evolution and maintenance of technological solutions for the digital infrastructure of national defense must be guaranteed (Pereira, B., 2022).

In terms of personnel, in 2023, the Cyber Academia and Innovation Hub (CAIH) was created, with the mission to establish activities of public interest aiming to promote education, training, and exercises, as well as to stimulate research, development, and innovation in the field of cyberspace, to foster necessary knowledge and skills for a new generation of professionals in cybersecurity and cyber defense (Portugal, 2023).

Additionally, the *Direção Geral dos Recursos Humanos da Defesa Nacional* (General Directorate of Human Resources of National Defense) developed an HR policy for cyber defense to meet the needs of recruitment, training, and retention of civilians or military personnel to act, mainly, as: cyber defenders, operators, forensic analysts, or cyber defense programmers (Pereira, B., 2022).

Within the scope of military higher education, training in cyber defense was initially developed at the Military Academy with a postgraduate degree in cyber defense and cybersecurity, followed by the Naval School with a Masters's Degree in Information Security and Cyberspace Law and the Portuguese Joint Command and Staff College, which also developed education and training in the field (Pereira, B., 2022).

Internationally, multilateral cooperation activities date back to 2013, when Portugal took the lead in NATO's Multinational Cyber Defense Education and Training (MN CD E&T). The goal was to create a platform for coordinating education and training in cyber defense and design new initiatives, contributing to the development of the area and interoperability within NATO.

In 2017, Portugal joined OTAN's Cooperative Cyber Defence Center of Excellence (CCDCOE), designed to boost training, education, and skills within the cyber defense domain. And, in 2019, the main headquarters of the Communications and Information Academy (NCI Academy), which brings together all the activities associated with the education and training provided by the Agency, especially those related to cyberspace.

Portugal also participates in exercises such as Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise (CWIX), an annual exercise designed to enhance interoperability between Alliance members and partner nations, and the Cyber Coalition, one of the largest cyber defenses in the world.

5 CONCLUSION

Throughout this article, we observed the growing effort the cyber sector conquered in the organization of Portugal's defense. Although guiding documents of the country's strategic planning date back to 2014 and need to be promptly updated, it appears that defensive and offensive actions in this area were already considered at that time to ensure national interests.

Considering the recently-approved proposal aimed at drafting a new CEDN—similar to the LPMs of 2019 and 2023 in which the sector received greater budget allocation—promoting cyberspace side by side with initiatives to produce specific strategic documents and organizational reforms, with emphasis on the creation of COCiber. These are important indicators, showing that the cyber domain gained strategic prominence in present and future operations.

Sharing of training, exercises, and data, as well as the training and retention of qualified personnel, in addition to investments in cutting-edge technologies, are indispensable elements for strategic defense planning in a context where the Armed Forces must be prepared to act in an interoperable manner and in multiple domains. Thus, cyber capacity is crucial, in times of war and peace, for countries' security and prosperity.

Portugal has undoubtedly taken crucial steps in recent years in its cyber defense survey, although it still must overcome important obstacles, such as the non-execution of the planned investment in 2022 to train the Cyber Defense Center, which continues to fall short of the needs in qualitative and quantitative terms and the significant delay in the creation of the Cyber Defense School. These facts raise expectations for a new cycle of strategic defense planning.

REFERENCES

ABREU, M. das N. **O Planeamento de Longo Prazo e a Renovação de Sistemas de Armas para o Período 2020-2035**. Trabalho de Investigação Individual do CPOG 2017/2018. Pedrouços: Instituo Universitário Militar, 2018.

ADAMSKY, D. **The Culture of Military Innovation**: The impact of cultural factors on the revolution in military affairs in Russia, the US, and Israel. Stanford: Stanford University Press, 2010.

COHEN, R.; CHANDLER, N.; EFRON, S.; FREDERICK, B.; HAN, E.; KLEIN, K.; MORGAN, F.; RHOADES, A.; SHATZ, H.; SHOKH, Y. **The Future of Warfare in 2030**. Santa Monica: Rand Corporation, 2020.

CONSELHO DE REVISÃO DO CONCEITO ESTRATÉGICO DE DEFESA NACIONAL. **Ciclo de Revisão do Conceito Estratégico de Defesa Nacional 2022-2023**. Lisboa: Ministério da Defesa da Defesa Nacional, 2023. Available at: https://www.idn.gov.pt/pt/noticias/Paginas/Ciclo-de-Revis%C3%A3o-do-Conceito-Estrat%C3%A9gico-de-Defesa-Nacional.aspx. Access on: Oct. 23, 2024.

DAEHNHARDT, P.; GASPAR, C. Portugal e a Revisão do Conceito Estratégico da NATO. **Relações Internacionais**, [*s. l.*], v. 67, p. 75-88, 2020. Available at: https://novaresearch.unl.pt/en/publications/portugal-e-a-revis%C3%A3o-do-conceito-estrat%C3%A9gico-da-nato. Access on: Oct. 23, 2024.

DAEHNHARDT, P. A Resposta da NATO à Nova Ordem Euro-Atlântica Confrontacional. **IDN Brief**, [*s. l.*], p. 1-2, 2022. Available at: https://run.unl.pt/handle/10362/167738?mode=full. Access on: Oct. 23, 2024.

DIÁRIO DA REPÚBLICA. **Despacho nº13692/2013**. Orientação Política para a Ciberdefesa. Lisboa: Ministério da Defesa Nacional, 2013.

DIÁRIO DA REPÚBLICA. **Resolução do Conselho de Ministros nº36/2015**. Aprova a Estratégia Nacional de Segurança do Ciberespaço. Lisboa: Presidência do Conselho de Ministros, 2015.

DIÁRIO DA REPÚBLICA. **Resolução do Conselho de Ministros nº92/2019**. Presidência do Conselho de Ministros. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, Lisboa: Ministério da Defesa Nacional, 2019.

DIÁRIO DA REPÚBLICA. **Despacho nº10309/2022**, Parte C, nº163, p.35-36, Gabinete da Ministra. Lisboa: Ministério da Defesa Nacional, 2022a.

DIÁRIO DA REPÚBLICA. **Resolução do Conselho de Ministros nº106/2022**. Presidência do Conselho de Ministros. Aprova a Estratégia Nacional de Ciberdefesa. Lisboa: Ministério da Defesa Nacional, 2022b.

FERNANDES, P. M. **O Conceito Estratégico da NATO (2010): A Perspectiva Portuguesa**. 2013. Tese (Mestrado) - Universidade Nova, Lisboa, 2013.

GARCIA, F. P. O Novo Conceito Estratégico da NATO. **IDN Brief**, [*s. l.*], 2022. Available at: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Access on: Nov. 2024.

GASPAR, C. O Conceito Estratégico de Madrid. **IDN Brief**, [*s. l.*], 2022. Available at: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Access on: Nov. 2024.

GERRING, J. Mere Description. **British Journal of Political Science**, Cambridge, v. 42, n. 4, p. 721-746, 2012. DOI: https://doi.org/10.1017/S0007123412000130

MARCELINO, V. Ciberdefesa volta à estaca zero. EMGFA vai agora abrir concurso público internacional. **Diário de Notícias**, Lisboa, 2023. Available at: https://www.dn.pt/edicao-do-dia/01-mai-2023/ciberdefesa-volta-a-estaca-zero-emgfa-vai-agora-abrir-concurso-publico-internacional-16262021.html. Access on: Aug. 2024.

NUNES, P. V. **A Edificação da Capacidade de Ciberdefesa Nacional**. 2020. Trabalho (Investigação Individual do CPOG 2019/2020) - Instituto Universitário Militar, Pedrouços, 2020.

NUNES, P. V. **Sociedade em Rede, Ciberespaço e Guerra de Informação**. Contributos para o Enquadramento e Construção de uma Estratégia Nacional da Informação. 2. ed. Lisboa: Instituto da Defesa Nacional, 2016.

NUNES, P. V. Estratégia Nacional de Ciberdefesa. *In*: NUNES, P. (coord.). **IDN Cadernos**. Contributos para uma Estratégia Nacional de Ciberdefesa. Lisboa: Instituto de Defesa Nacional, 2018.

OTAN - Organização do Tratado do Atlântico Norte. Wales Summit Declaration Press Release. **OTAN**, Bruxelas, 2014. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm. Access on: Aug. 2024.

OTAN - Organização do Tratado do Atlântico Norte. Strategic Concept. **NATO Summit**, Madrid, 2022. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. Access on: Aug. 2024.

PEREIRA, B. da S. **A Evolução da Relevância do Ciberespaço para a NATO**. 2022. Trabalho (Investigação Individual do CEMC 2021/22) - Instituto Universitário Militar, Pedrouços, 2022.

PEREIRA, R. A. **Desenvolvimento da Capacidade de Ciberdefesa Destacável (NATO CD-DEPLOY)**. 2022. Trabalho (Investigação Individual CPOS-FA 2021/22) - Instituto Universitário Militar, Pedrouços, 2022.

PINHO, P. **O Modelo de Ciberdefesa Nacional: Solução Centralizada ou Distribuída?** 2020. Trabalho (Investigação Individual do CPOS-M) - Instituto Universitário Militar, Pedrouços, 2020.

PIRES, N. de L. **O Novo Conceito de "Multi-Domain Battle" e suas implicações na edificação de capacidades militares no Exército**. 2018. Trabalho (Investigação Individual do CPOG 2017/18) - Instituto Universitário Militar, Pedrouços, 2018.

PORTUGAL. **Conceito Estratégico de Defesa Nacional**. Lisboa: Ministério da Defesa Nacional, 2013a. Available at: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf. Access on: June 2023

PORTUGAL. **Resolução do Conselho de Ministros n. 26/2013 de 11 de abril**. Defesa 2020. Lisboa: Ministério da Defesa Nacional, 2013b. Available at: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Defesa-2020.pdf. Access on: Aug. 2024

PORTUGAL. Ministério da Defesa Nacional. **Despacho n. 13692/2913**. Orientação para a política de Ciberdefesa. Diário da República, n. 208. Lisboa: Ministério da Defesa Nacional, 2013c. Available at: https://diariodarepublica.pt/dr/detalhe/despacho/13692-2013-3295679. Access on: Aug. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Resolução do Conselho de Ministros n. 36/2015, de 12 de junho**. Estratégia Nacional de Segurança do Ciberespaço. Diário da República n. 113/2015. Lisboa: Ministério da Defesa Nacional, 2015. Available at: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/36-2015-67468089. Access on: Aug. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Resolução do Conselho de Ministros n. 92/2019 de 5 de junho**. Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Lisboa: Governo de Portugal, 2019.

PORTUGAL. **Despacho n. 2536/2020**. Diretiva Ministerial de Planeamento de Defesa Militar – quadriénio 2019-2022. Diário da República n. 38/2020. Lisboa: Ministério da Defesa Nacional, 2020. Available at: https://diariodarepublica.pt/dr/detalhe/despacho/2536-2020-129529718. Access on: Aug. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Resolução do Conselho de Ministros n. 106/2022, de 2 de novembro**. Estratégia Nacional de Ciberdefesa. Diário da

República n. 211/2022. Lisboa: Ministério da Defesa Nacional, 2022a. Available at: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924. Access on: Aug. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Decreto-Lei n. 19/2022, de 24 de janeiro**. Lei Orgânica do Estado-Maior-General das Forças Armadas. Diário da República n. 16/2022. Lisboa: Ministério da Defesa Nacional, 2022b. Available at: https://diariodarepublica.pt/dr/detalhe/decreto-lei/19-2022-178080766. Access on: Aug. 2024.

PORTUGAL. Presidência do Conselho de Ministros. **Decreto-Lei n. 34/2023, de 23 de maio**. Cyber Academia and Innovation Hub. Diário da República n. 99/2023. Lisboa: Ministério da Defesa Nacional, 2023. Available at: https://diariodarepublica.pt/dr/detalhe/decreto-lei/34-2023-213345452. Access on: Aug. 2024.

PORTUGAL. **O Centro de Ciberdefesa**, s.d. Available at: https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro. Access on: Aug. 2024.

REIS, B. C. **Pode Portugal ter uma estratégia?** Lisboa: Fundação Francisco Manuel dos Santos, 2019.

REIS, B. C. Uma Nova Estratégia para a NATO vista de Portugal. **IDN Brief**, [*s. l.*], 2022. Available at: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Access on: Nov. 2024.

RODRIGUES, Alexandre Reis. Considerações sobre o Sistema de Forças Nacional. **Cadernos Navais**, Lisboa, n. 5, p. 1-70, 2003.

RODRIGUES, A. R. **O pensamento de Defesa em Portugal**. Lisboa: Edições Culturais da Marinha, 2020.

SCHWETHER, N. A Guerra do Futuro: comparação das estratégias adotadas pelos Exércitos de Estados Unidos, Espanha e Israel. **Análise Estratégica**, Brasília, DF, v. 21, n. 3, p. 117-149, 2021. Available at: http://www.ebrevistas.eb.mil.br/CEEExAE/article/view/8496. Access on: Oct. 24, 2024.

SERRA, M. Até ao fim do ano, Portugal vai quadruplicar os efetivos militares dedicados à ciberdefesa. **TSF Rádio Notícias**, Lisboa, abr. 2019. Available at: https://www.tsf.pt/politica/ate-ao-fim-do-ano-portugal-vai-quadruplicar-os-efetivos-militares-dedicados-a-ciberdefesa-10756302.html. Access on: Oct. 2021.

SERRONHA, M. Portugal e o Novo Conceito Estratégico da NATO. **Relações Internacionais**, [*s. l.*], v. 27, p. 55-66, 2010.

STORTI, D., FERREIRA, M. O Estado como agente inovador nas revoluções nos assuntos militares (RAMs). *In*: ENCONTRO NACIONAL DA ASSOCIAÇÃO BRASILEIRA DE ESTUDOS DE DEFESA, 12., 2022, Niterói. **Anais** [...]. ABED, Niterói, 2022. Available at: https://www.enabed2022.abedef.org/resources/anais/19/enabed2022/1658704156_ARQUIVO_c9ff3811d484366195230218744486f8.pdf. Access on: Aug. 2024.