ARTIGO DOI 10. 52781/cmm.145

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

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

Abstract: This article understands 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, the exploration and global analysis of strategic documents from the government and the Portuguese Armed Forces is adopted, which allow us to understand in greater depth the dynamics of the case. The study reveals the prioritization and attention recently conquered by the cyber domain in the country, with significant actions such as the creation of the Cyberdefense Operations Command.

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

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

Recibido: 7 jun. 2023
Aprobado: 27 sep. 2024

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

* Este trabajo contó con el apoyo de la Coordinación para el Mejoramiento del Personal de Educación Superior –Brasil (CAPES)– Código de Financiamiento 001ível Superior – Brasil (CAPES) – Código de Financiamento 001

1 INTRODUCCIÓN

En la última década hemos observado un aumento de la relevancia del ciberespacio para la planificación estratégica de los Estados y sus respectivas Fuerzas Armadas. En el marco de la Organización del Tratado del Atlántico Norte (OTAN), los Jefes de Estado y de Gobierno de los Estados miembros anunciaron en 2014 que la ciberdefensa era uno de los objetivos de defensa colectiva del grupo y que había la necesidad de mejorar las capacidades en este ámbito (OTAN, 2014).

Más tarde, en 2016, los Aliados reconocieron formalmente el ciberespacio como el cuarto dominio de las operaciones militares. Y, más recientemente en 2022, el Concepto Estratégico de la OTAN reafirmó que el uso seguro y el acceso sin restricciones al ciberespacio son fundamentales para una efectiva disuasión y defensa colectiva (OTAN, 2022).

En el marco de la Unión Europea (UE), la ciberdefensa también es un campo prioritario. En 2020, la Estrategia de Ciberseguridad de la Unión Europea afirmó que el ciberespacio era un dominio de la actividad militar. Y, en 2022, la Brújula Estratégica se comprometió a desarrollar una política para el sector.

Portugal, Estado del sur de Europa, miembro de la Comunidad Económica Europea desde 1986 y miembro fundador de la Alianza Atlántica, también se ha dedicado a desarrollar un conjunto de iniciativas para garantizar el uso libre y seguro del ciberespacio (Pinho, 2020).

Entre ellas se encuentran el Concepto Estratégico de Defensa Nacional (2013) –que determinó el delito cibernético como uno de los principales riesgos para la seguridad nacional–; la definición de una Orientación Política para la Ciberdefensa (2013); la creación del Centro de Ciberdefensa (CCD) de las Fuerzas Armadas (2014) y del Centro de Ciberseguridad – CNCS– (2014); la Estrategia Nacional de Ciberseguridad (2015 y 2019); y la Estrategia Nacional de Ciberseguridad (2022).

En este contexto, el Ministerio de Defensa consideró la ciberdefensa como uno de los proyectos prioritarios de su acción y afirmó que es imperativo cualificar los recursos humanos asignados al área (Orden 10309/2022).

Por lo tanto, este artículo pretende 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? Este contexto tiene en cuenta la constante evolución de la guerra, que se desarrolla de manera impredecible, sumada a la expansión del campo de batalla cubriendo una amplia variedad de dominios y medios (cibernético, espacial, cognitivo e informativo) para ser utilizados posiblemente por los adversarios en el futuro ámbito operativo (Schwether, 2021).

Para ello, se utilizará la investigación exploratoria, que, al describir los principales documentos estratégicos portugueses producidos en la última década, nos permite comprender las etapas de la planificación de la defensa y, en particular, cómo ha evolucionado y se ha organizado el sector cibernético.

Se requiere la descripción al responder preguntas relacionadas a cuándo, quién y cuál. La calidad inferencial de una descripción está directamente relacionada con la calidad de las fuentes de datos, de los instrumentos de medición o de los procedimientos de codificación (Gerring, 2012).

En este contexto, a esta introducción le siguen tres secciones. En la primera sección se aborda lo que aquí llamamos una gran estrategia, es decir, un plan con una visión holística y multidimensional

de las prioridades de acción del Estado (Reis, 2019). En la segunda sección, la atención se centra en el sistema de planificación estratégica de las Fuerzas Armadas portuguesas, recopilando los principales documentos que guían la construcción de capacidades futuras. En la tercera sección, el alcance del análisis se reduce a la capacidad cibernética y su evolución a nivel estratégico y organizativo. Y la conclusión cierra con reflexiones sobre los importantes avances realizados y los obstáculos que aún quedan por enfrentar.

2 GRAN ESTRATEGIA

La alianza estratégica transatlántica entre Estados Unidos, Canadá y Europa fue institucionalizada por el Tratado del Atlántico Norte en 1949. Desde entonces, esta relación ha sido fundamental para establecer las estrategias y políticas de defensa y seguridad de Europa, así como un instrumento esencial para la afirmación de la política exterior portuguesa.

El concepto estratégico (CE) es uno de los documentos fundamentales formulados por la OTAN que presenta la visión estratégica para el futuro. Desde 1991, este documento ha definido públicamente las prioridades estratégicas de la Alianza y proporcionado una orientación importante para las instituciones militares de los 32 Estados miembros. Así, la importancia de que los intereses nacionales portugueses expresen los grandes principios comunes acordados y de que la planificación nacional abarque esta publicación (Reis, 2022; Serronha, 2010).

El CE aprobado a finales de 2010 en Lisboa se centró en tres cuestiones: defensa colectiva, gestión de crisis y seguridad cooperativa. Uno de los puntos más relevantes de este documento trata sobre la extensión del ámbito de acción de la Organización, es decir, si un miembro está en riesgo, la Alianza puede actuar fuera de sus propias fronteras. También expresó un propósito de participación activa en la seguridad internacional al proponer alianzas con otros países y organizaciones (Fernandes, 2013).

Sin embargo, en cuanto a la política exterior portuguesa, el documento ya no incorpora varios temas de interés de la diplomacia del país, especialmente en lo que respecta a la expansión de las asociaciones hacia el Atlántico Sur (Fernandes, 2013). La vocación marítima de Portugal contribuye para la afirmación del país en el contexto internacional, y el Atlántico es una zona de interés estratégica.

Después de diez años de la aprobación del último CE y en un contexto de creciente digitalización de la sociedad y complejidad del contexto global de seguridad y defensa, se dio inicio a otro proceso formal de revisión del documento.

El CE de Madrid, aprobado en 2022, al mismo tiempo que reafirma los principios básicos de la Organización[1], también presenta una nueva lista de posibles adversarios, con la inclusión de China y Rusia. Además, destaca el surgimiento de nuevas tecnologías y el creciente interés por los dominios espacial y cibernético (Daehnhardt; Gaspar, 2020; Gaspar, 2022; Garcia, 2022; Daehnhardt, 2022).

El CE es uno de los principales insumos para la formulación del Concepto Estratégico de Defensa Nacional (CEDN) en Portugal. El CEDN es el principal instrumento que presenta la estrategia nacional de defensa y seguridad y una herramienta que coordina los esfuerzos de las diversas agencias estatales para mitigar las preocupaciones nacionales[2] (Portugal, 2013a).

1 La defensa colectiva y la disuasión son principios centrales.

2 Estas son el terrorismo, la proliferación de armas de destrucción masiva, la delincuencia organizada transnacional, la ciberdelincuencia y la piratería.

El documento, aprobado en 2013, recomienda que las Fuerzas Armadas realicen una acción conjunta con la participación de todos los ámbitos de la institución desde conceptos, doctrinas, procedimientos hasta la cultura institucional y organizacional. Además, propone una reorganización y simplificación de las estructuras, con vistas a una mayor eficiencia, agilidad, modularidad y flexibilidad. En el ámbito de la planificación estratégica, el CEDN determinó que las inversiones se orientaran hacia las capacidades necesarias para cumplir las misiones prioritarias (Portugal, 2013a).

Respecto al entorno cibernético, se esbozaron algunos objetivos, incluidos la definición de una Estrategia Nacional de Ciberseguridad, la creación de organismos técnicos, la sensibilización de los usuarios y la mejora de la capacidad nacional de ciberdefensa. Para ello, es urgente una mejor comunicación estratégica de las Fuerzas Armadas y el fomento de la investigación y la innovación (Portugal, 2013a).

En conclusión, aunque el componente tecnológico es frecuentemente una condición inicial importante para las innovaciones, una verdadera revolución militar depende de la confluencia entre armas, operaciones, organización y visión de la guerra en el futuro (Adamsky, 2010). Tan importante como el papel del Estado como agente impulsor, capaz de invertir en la investigación, es la definición de áreas prioritarias y formulación de estrategias a largo plazo (Storti; Ferreira, 2022).

En otras palabras, a medida que el futuro de la guerra requiere más demandas y mueve los recursos limitados de los Estados en direcciones opuestas, los Estados son los responsables de tomar las grandes decisiones estratégicas (Cohen *et al*., 2020).

Así, dadas las repercusiones de la crisis pandémica, sumada al fin de la paz en el continente europeo, en 2022 se volvió necesario empezar un proceso de revisión del CEDN impulsado por un conjunto de iniciativas para promover el debate público sobre los temas de interés y por personalidades de reconocido mérito, quienes se reunieron para reflexionar sobre los temas (Conselho, 2023).

En 2023 se dio a conocer el Informe de Revisión del Concepto Estratégico de Defensa Nacional. La propuesta, aprobada en mayo, forma parte del proceso de revisión del CEDN e integrará la versión final, que será aprobada por la resolución del Consejo de Ministros, por el primer ministro y por el ministro de Defensa Nacional.

En el documento, la disputa sobre el dominio del ciberespacio y la expansión de las capacidades cibernéticas de los actores estatales y no estatales se identificaron como desafíos para la estabilidad y la seguridad estratégicas. Además de la competencia en el ciberespacio y la sofisticación de los ataques y los daños que pueden provocar, especialmente, en las infraestructuras críticas, la disputa se consideró una de las mayores amenazas, difícil de anticipar y susceptible de afectar a las funciones sociales básicas y al bienestar de los ciudadanos (Conselho, 2023).

También afirmó categóricamente que es esencial mejorar las capacidades de defensa y resiliencia del país, además de fortalecer la cooperación en defensa, aumentar la capacidad de la industria militar y fortalecer las capacidades de las Fuerzas Armadas, asegurando las estructuras y mecanismos necesarios para la acción integrada en los diferentes dominios operativos (Conselho, 2023).

Más específicamente, en el documento se recomendó el desarrollo de la capacidad nacional en el ámbito del espacio y del ciberespacio, y la planificación de la adquisición de nuevos medios, equipos y sistemas para construir a mediano y largo plazos, todo el espectro de las

capacidades militares. Esto se da en paralelo a la valorización y cualificación de la dimensión humana de las Fuerzas, profundizando en el proceso de profesionalización del sistema militar (Conselho, 2023).

Los analistas sugirieron horizontes temporales más cortos para la revisión, la implementación de mecanismos para monitorear acciones, como un cambio en el nombre del documento, del Concepto Estratégico de Defensa Nacional a Estrategia de Seguridad y Defensa. En el futuro, el documento podría sentar las bases para una Estrategia Nacional de Seguridad (Conselho, 2023)[3].

3 PLANIFICACIÓN ESTRATÉGICA EN DEFENSA

Portugal tiene un sistema de planificación estratégica que, en sus aspectos esenciales, se ha mantenido aproximadamente cuatro décadas sin cambios. Creado en los años 1980, se buscó desarrollar el sistema secuencial y jerárquicamente en varias fases, que empieza por el CEDN (abordado en la sección anterior), seguido del Concepto Estratégico Militar (CEM), la definición de las Misiones de las Fuerzas Armadas (MIFA), del Sistema de Fuerzas Nacionales (SF) y el Dispositivo de Fuerzas (Rodrigues, 2020).

Figura 1. Planeamiento Estratégico de Defensa

Fuente: Elaboración propia, 2023.

El CEM identifica, entre otras acciones, los objetivos militares estratégicos, las modalidades de acción militar para lograrlos y proporciona recomendaciones en términos de medios. Es responsabilidad del Ministerio de Defensa Nacional conforme propuso el Consejo de Jefes de Estado Mayor (Rodrigues, 2020).

Hasta su revisión, el documento aprobado en 2014 es el principal instrumento nacional que orienta la construcción de capacidades futuras, según los contextos de empleo, objetivos militares

3 La propuesta está en consonancia con la perspectiva de Rodrigues (2020), quien señala que lo que se considera en Portugal como CEDN es, de hecho, una estrategia y no un concepto, y, por lo tanto, debe garantizar una armonía entre los objetivos y los medios. Un concepto operativo es esencialmente la formulación de una idea sobre cómo se puede hacer o lograr algo y que, por lo tanto, puede conducir a un determinado procedimiento o capacidad. Los conceptos suelen ser una visión de cómo las Fuerzas Armadas pretenden operar en el mediano y largo plazos, en función de los cambios observados en el escenario o en los dominios estratégicos. Los conceptos suelen contener elementos resultantes de la combinación de una evaluación informada y el pensamiento innovador (Nunes, 2016).

y niveles de ambición definidos en él. Específicamente en casos de ciberataques, instruye que las Fuerzas Armadas serán llamadas a intervenir para:

> [...] garantizar la salvaguarda de su información y la protección de sus infraestructuras de comunicaciones y sistemas de información, apoyar la protección y defensa de las infraestructuras críticas nacionales, así como colaborar con otras instituciones estatales en el ámbito de la ciberseguridad, contribuyendo a la protección de las poblaciones y la promoción de su bienestar (Portugal, 2023).

Además, señala la preocupación por obtener capacidades diversificadas, interoperables e integrables, así como la intención de organizar las Fuerzas Armadas con énfasis en el uso modular, flexible, conjunto y combinado. Aunque cabe destacar que la ausencia de un horizonte temporal definido hace que las indicaciones sean inexactas para la planificación a largo plazo de las Fuerzas Armadas (Abreu, 2018; Pires, 2018).

Las MIFA tienen por objetivo identificar las misiones a nivel estratégico y militar asignadas a las Fuerzas Armadas y que corresponden a misiones militares específicas. La ejecución de las misiones respeta las prioridades y lineamientos que constan en el CEDN y en el CEM.

En las MIFA presentadas en 2014, las misiones se centran en seis áreas: (a) seguridad y defensa del territorio nacional y de los ciudadanos; (b) defensa colectiva; (c) ejercicio de la soberanía, jurisdicción y responsabilidades nacionales; (d) seguridad cooperativa; (e) apoyo al desarrollo y bienestar; y (f) cooperación y asistencia militar.

Para la defensa del territorio nacional se prevé la posibilidad de:

> [...] aplicar medidas defensivas y, si necesario, ofensivas contra los ciberataques**,** con el fin de garantizar la salvaguarda de la información y la protección de las infraestructuras de Comunicaciones y Sistemas de Información de las Fuerzas Armadas, así como el apoyo en la protección y defensa de las infraestructuras críticas nacionales y electrónicas del gobierno del Estado (Portugal, 2014, p. 3, énfasis añadido).

El SF identifica un conjunto de capacidades requeridas para cumplir con las misiones de las Fuerzas Armadas, indicando los tipos y cantidades de fuerzas y medios con base en directrices específicas, contextos de uso y complementariedad operativa.

El documento, sin embargo, no sirve de referencia para el desarrollo de programas y para el reequipamiento militar porque se limita a una lista de unidades, infraestructuras, organismos, etc. y no presenta una visión de futuro ni anticipa las necesidades de modernización (Rodrigues, 2003).

Por otro lado, el Dispositivo de Fuerzas establece la relación entre los comandos operacionales, las Fuerzas, las unidades y los medios con las infraestructuras que los soportan, materializando la forma en que están organizados y responden a diversas capacidades enumeradas en el SF para cumplir con las MIFA.

Finalmente, la Ley de Programación Militar (LPM) es el instrumento financiero para materializar la estrategia militar capaz de dotar a las Fuerzas Armadas de las capacidades militares

necesarias para llevar a cabo sus misiones en lo que respecta a los materiales –mantenimiento, sustitución o innovación– (Abreu, 2018).

Entre los proyectos incluidos en la LPM se encuentra la defensa cibernética; sobre todo, la protección y seguridad de las redes informáticas de infraestructuras críticas y los sistemas de Comando y Control y la provisión de capacidad ofensiva a las Fuerzas Armadas para neutralizar posibles amenazas. Una comparación entre las LPM de 2015 y 2019 indicó un importante incremento de las inversiones dirigidas al sector y al mantenimiento de recursos para el período 2023-2034[4].

Aunque cabe destacar que el presupuesto para la ciberdefensa no llegó a más del 50%[5], ya sea por la pandemia, por la escasez de recursos humanos especializados o por el retraso en la tramitación de los casos (Marcelino, 2023).

Además, el ciclo de planificación estratégica 2014-2019 se guio por el documento Reforma de Defensa 2020 de abril de 2013, que consideraba instaurar Fuerzas Armadas más modernas, operativas, sostenibles y eficientes. Las directrices se dividieron en dos pilares: (i) nuevo ciclo de planificación estratégica y (ii) reorganización de la macroestructura. En cuanto a la estructura, se valoró la naturaleza conjunta, modular y flexible. Entre las directrices específicas destaca un incremento de la capacidad de ciberdefensa (Portugal, 2013b).

Más recientemente, la Directiva Ministerial sobre Planificación de la Defensa Militar, cuadrienio 2019-2022, aprobada en 2020 continuó por reforzar la dimensión de comando conjunto de las Fuerzas y la relevancia de integrar eficazmente los componentes terrestre, naval y aéreo, así como las capacidades de actuación en el ciberespacio (Portugal, 2020).

Además, enfatizó el compromiso de pensar en la defensa nacional; más específicamente, la renovación de la estructura, la doctrina y los medios, a la luz de nuevos desafíos como, por ejemplo, el espacio y el ciberespacio, la inteligencia artificial y la desinformación. Esto se realiza teniendo en cuenta la frecuencia y la creciente intensidad de los ciberataques y el reto de los nuevos actores, de las nuevas tecnologías y de los nuevos dominios (Portugal, 2020).

4 ACCIONES EN EL CIBERESPACIO

La primera iniciativa a nivel estratégico se llevó a cabo en 2013 con la promulgación de la Directriz Política para la Ciberdefensa, un documento que sienta las bases para desarrollar capacidades en el sector.

Este documento estableció tres objetivos principales: (i) garantizar la protección, la resiliencia y la seguridad de las redes de contraataque; (ii) la libertad de acción del país en el ciberespacio: garantizar y, cuando sea necesario, prevenir u obstaculizar su uso hostil contra el interés nacional; y (iii) contribuir de manera colaborativa en el contexto nacional (Portugal, 2013c).

Para lograr estos objetivos, se definieron siete líneas de acción: (1) establecimiento de la estructura nacional de ciberdefensa; (2) integración de las operaciones del ciberespacio en el ámbito de las capacidades militares; (3) llevar a cabo todo el espectro de operaciones militares en

4 LPM 2015-2026 recursos totales para Ciberdefensa 14.000; LPM 2019-2030 recursos totales para Ciberdefensa 45.490; LPM 2023-2034 recursos totales para Ciberdefensa 43.469.

5 En 2020 solo el 48,9%; en 2021 bajó al 27%; y en 2022 fue del 30,7% (Marcelino, 2023).

el ciberespacio; (4) fortalecer la capacidad de información en el ciberespacio; (5) desarrollar un sistema de alerta inmediato y de intercambio de información a varios niveles y ámbitos de decisión; (6) promover una cultura de gestión de riesgos mediante la incorporación de requisitos de gestión de riesgos en las adquisiciones por realizar y en la cadena de suministro; y (7) centralizar la formación y capacitación en ciberdefensa y adaptar la gestión de los recursos humanos para asegurar su permanencia en estas actividades (Portugal, 2013c).

El documento también identificó la necesidad de establecer asociaciones entre las instituciones estatales y las privadas, nacionales e internacionales, como una forma de promover el desarrollo tecnológico, la investigación y la innovación (Portugal, 2013c).

En 2015, la ciberdefensa logró ser mejor definida con la publicación de la Estrategia Nacional de Seguridad del Ciberespacio (ENSC). La Estrategia tuvo como objetivo profundizar en la seguridad de las redes y de los sistemas de información, además de permitir un uso libre, seguro y eficiente del ciberespacio (Portugal, 2015).

Con este fin, se definieron seis ejes de intervención, a saber: Eje 1: Estructura de seguridad del ciberespacio; Eje 2: Lucha contra la ciberdelincuencia; Eje 3: Protección del ciberespacio y las infraestructuras; Eje 4: Educación, sensibilización y prevención; Eje 5: Investigación y desarrollo; Eje 6: Cooperación. Del primer eje es posible obtener funciones específicamente asignadas a la defensa nacional, a saber:

> a) Implementar la Orientación Política para la Ciberdefensa, aprobada por Orden 13692/2013, de 11 de octubre, publicada en la Gaceta Oficial n.º 208, serie 2, de 28 de octubre, construyendo la estructura nacional de ciberdefensa;
>
> b) Establecer y consolidar una estructura de comando y control para la ciberdefensa nacional [...];
>
> c) Implementar, desarrollar y consolidar la capacidad de ciberdefensa, con miras a asegurar la realización de operaciones militares en el ciberespacio, asegurar la libertad de acción del país en el ciberespacio y, cuando sea necesario y determinado, la explotación proactiva del ciberespacio para prevenir u obstaculizar su uso hostil contra el interés nacional;
>
> d) Constituir la ciberdefensa como un área en que es necesario promover sinergias y potenciar el doble uso de sus capacidades en el ámbito de las operaciones militares y la ciberseguridad nacional, desarrollando y consolidando un sistema de intercambio de información a diversos niveles y ámbitos de decisión (Portugal, 2015, énfasis añadido).

Por último, el documento subrayó la importancia de realizar una revisión constante y periódica en un plazo máximo de tres años, así como de llevar a cabo una verificación anual de los objetivos estratégicos y de las líneas de acción a la luz de la evolución de las circunstancias (Portugal, 2015).

En 2019 se aprobó la segunda Estrategia Nacional de Seguridad del Ciberespacio de Portugal, basada en tres objetivos estratégicos: maximizar la resiliencia, promover la innovación

y generar y garantizar recursos, que dieron como resultado seis ejes de intervención, muy similares a los de la versión anterior (Portugal, 2019).

Con respecto a la ciberdefensa, buscó fortalecer la resiliencia de las Fuerzas Armadas, para lo cual se deben utilizar todos los medios para responder a los ciberataques incluida la capacidad ofensiva. Al mismo tiempo, se pretendía maximizar la seguridad y la defensa de las redes y sistemas de información mediante la capacidad de ciberdefensa (Portugal, 2019).

También refiere a la necesidad de profundizar en el doble uso de las capacidades de ciberdefensa, desarrollando y consolidando un sistema de intercambio de información en varios niveles y ámbitos de decisión. Además, participa en ejercicios de ciberseguridad y ciberdefensa, teniendo en cuenta la cooperación internacional y la afirmación de Portugal en este campo (Portugal, 2019).

A raíz de la ENSC, y ante la necesidad de densificar conceptos a nivel estratégico y articular adecuadamente las estructuras orientadas al ciberespacio, en noviembre de 2022 se publicó la Estrategia Nacional de Ciberdefensa –ENCD– (Nunes, 2018).

La ENCD reafirma el ciberespacio como un dominio de las operaciones militares, defensivas y ofensivas; de las cuales estas últimas son exclusivas de las Fuerzas Armadas, como una forma de garantizar la defensa y los intereses nacionales, en respuesta a las amenazas provenientes de Estados o entidades no estatales y dependientes de la autorización política (Portugal, 2022a).

En este sentido, establece que el desarrollo de la capacidad cibernética debe estar en consonancia con los otros documentos rectores de la defensa militar; es decir, el ciberespacio es un elemento integral del proceso de planificación que valora una lógica de múltiples dominios y flexibilidad operativa, y las Fuerzas Armadas deben asegurar todas las capacidades de comando y control relevantes para este nuevo dominio (Portugal, 2022a).

También se definieron cuatro objetivos estratégicos: consolidar la capacidad de defensa cibernética; maximizar la resiliencia y la cohesión de la acción nacional; promover la investigación, el desarrollo y la innovación; y garantizar recursos calificados. Y seis ejes rectores para el plan de acción: Eje 1: utilizar el ciberespacio como dominio de operaciones; Eje 2: fortalecer la capacidad nacional de ciberdefensa; Eje 3: crear la escuela de ciberdefensa; Eje 4: intensificar la cooperación nacional e internacional; Eje 5: promover la investigación, el desarrollo y la innovación en el ciberespacio fomentando el desarrollo de soluciones de doble uso; Eje 6: garantizar las capacidades de ciberdefensa necesarias en contextos de estado de excepción (Portugal, 2022a).

Con respecto al desarrollo de capacidades, tres líneas de acción son prioritarias: aumentar el personal cualificado, contar con una infraestructura tecnológicamente avanzada, y garantizar la independencia tecnológica, promoviendo, por ejemplo, la industria 4.0. Una especial atención se centra en la captación, la selección, la retención y la formación del componente humano (Portugal, 2022a, Serra, 2019).

Incluso propuso la construcción de una entidad de formación en el ámbito de las Fuerzas Armadas y en colaboración con otras entidades de referencia nacional e internacional. También consideró importante la participación activa en mecanismos de gestión de crisis, en ejercicios y organizaciones internacionales que trabajan con la seguridad del ciberespacio (Portugal, 2022).

A nivel organizacional, en 2014 se creó el Centro de Ciberdefensa (CCD) de las Fuerzas Armadas. La concepción del CCD revela, hasta la fecha, la adecuación con el pensamiento estratégico de la institución. El CCD forma parte de la estructura del Estado Mayor General de las Fuerzas Armadas (EMGFA) y está conformado por los militares de las tres ramas; su misión principal es

garantizar la integridad, la confidencialidad y la disponibilidad de la información y de los sistemas de información de la defensa nacional (Portugal, s.d.).

Más recientemente, la Ley Orgánica del Estado Mayor General de las Fuerzas Armadas de 2022 cambió la estructura, hasta entonces destinada a la ciberdefensa. Con su aprobación, el EMGFA tuvo su misión ampliada, contemplando, además del uso de las Fuerzas Armadas en misiones y acciones operativas, la estrategia de defensa militar, la educación superior militar, la salud militar, la información y seguridad militar, la ciberdefensa, los aspectos militares del programa espacial de defensa nacional y la innovación y transformación en las Fuerzas Armadas (Portugal, 2022b).

Las nuevas competencias del EMGFA tienen como objetivo garantizar el principio fundamental de la unidad de comando y coordinación, así como seguir el proceso de adaptación de las Fuerzas Armadas para que puedan operar en los múltiples dominios y hacer frente a amenazas transnacionales e híbridas (Portugal, 2022b).

En el ámbito cibernético se crearon dos estructuras: el Centro de Comunicaciones e Información, Ciberespacio y Espacio (CCICE), directamente dependiente del Jefe del Estado Mayor General de las Fuerzas Armadas (CEMGFA), y el Comando de Operaciones de Ciberdefensa –COCiber– (Portugal, 2022b).

La misión del CCICE es habilitar la capacidad conjunta de Comando y Control de las Fuerzas Armadas, garantizar el ejercicio del comando de las operaciones militares en y a través del ciberespacio por parte del CEMGFA y orientar los aspectos militares del programa espacial de defensa nacional (Portugal, 2022b).

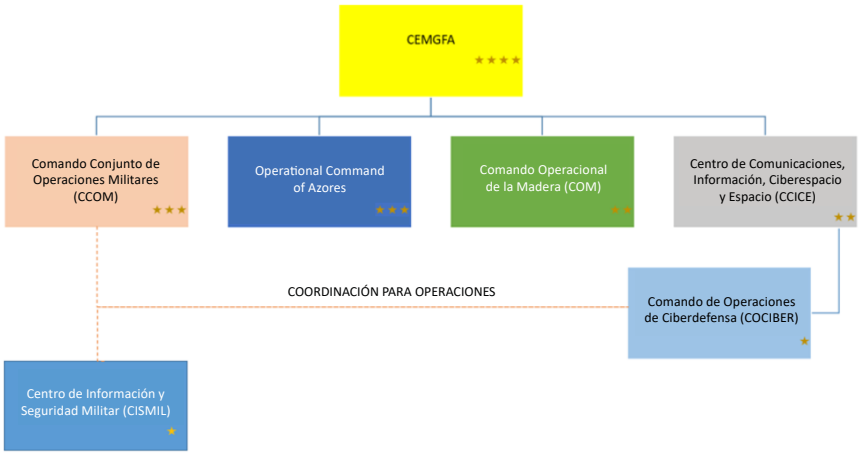
El CCICE es responsable de planificar, coordinar y ejecutar las medidas de seguridad de los sistemas de información y comunicaciones y la respuesta a incidentes para la protección y resiliencia de la infraestructura tecnológica conjunta, así como de proponer y realizar operaciones militares en y a través del ciberespacio en apoyo de objetivos militares, participar y organizar ejercicios conjuntos y combinados de ciberdefensa, proporcionar y coordinar la capacidad de ciberdefensa, actuar en articulación y estrecha cooperación con las estructuras nacionales responsables de la seguridad del ciberespacio. El organismo abarcará en su estructura la Escuela de Ciberdefensa –ECD– (Portugal, 2022b).

El COCiber es responsable de planificar, dirigir, controlar y ejecutar operaciones en y a través del ciberespacio. La estructura del COCiber puede ser reforzada por elementos o unidades de las ramas de las Fuerzas, así como para el desarrollo de operaciones y para la planificación y realización de ejercicios conjuntos o combinados. También está relacionado con las estructuras internacionales vinculadas a la ciberdefensa y la ciberseguridad dentro de la OTAN y la UE. Su estructura abarca la Fuerza de Operaciones de Ciberdefensa (Portugal, 2022b).

En cuanto a la ciberseguridad, cada Fuerza es responsable de la respuesta a incidentes de sus CIS, bajo la coordinación del COCiber. Cuando hay un incidente que la Fuerza no puede resolver de forma autónoma, el COCiber asume el control táctico, con la responsabilidad de dar una respuesta al incidente (Pereira, R., 2022b).

El COCiber tiene como objetivo contribuir a una mejor articulación operativa, para mejorar la coordinación entre el EMGFA y las ramas de las Fuerzas, y de prever una relación directa con el Comando Conjunto de Operaciones Militares (CCOM), lo cual acercará el ciberespacio a otros dominios de la guerra (Pereira, B., 2022).

Figura 2. Organigrama de Defensa



Fuente: Bruno Pereira (2022).

Por lo tanto, con la reestructuración de la capacidad cibernética, los componentes de ciberdefensa de cada Fuerza estaban bajo la esfera del COCiber, lo que permite una mayor interoperabilidad y otorga al Comando un papel central en la ciberdefensa nacional (Nunes, 2020).

En cuanto al vector material, el Plan de Desarrollo de Capacidades de Ciberdefensa (PDCCD) 2021-2021 establece que se debe garantizar la evolución y el mantenimiento de soluciones tecnológicas para la infraestructura digital de defensa nacional (Pereira, B., 2022).

En ámbito de personal, en 2023 se creó el *Cyber Academia and Innovation Hub* (CAIH), cuya misión fue desarrollar actividades de interés público orientadas a promover la formación, la capacitación y los ejercicios, así como estimular la investigación, el desarrollo y la innovación en el ámbito del ciberespacio. Esta acción permite fomentar los conocimientos y habilidades necesarias para una nueva generación de profesionales en el área de ciberseguridad y ciberdefensa (Portugal, 2023).

Más allá, la Dirección General de Recursos Humanos (RH) de la Defensa Nacional desarrolló una política de RH para la ciberdefensa, con la que pretende atender las necesidades de reclutamiento, de formación y de retención de personal civil o militar para actuar, principalmente, como ciberdefensores, operadores, analistas forenses o programadores de ciberdefensa (Pereira, B., 2022).

En el ámbito de la educación superior militar, la formación en ciberdefensa se desarrolló inicialmente en la Academia Militar con un Posgrado en Ciberdefensa y Ciberseguridad, seguida de la Escuela Naval, con una Maestría en Seguridad de la Información y Derecho en el Ciberespacio, y del Instituto Universitario Militar, que también desarrolló formación y capacitación en el campo (Pereira, B., 2022).

En el ámbito internacional, las actividades de cooperación multilateral se remontan a 2013, cuando Portugal tomó la iniciativa en el proyecto *Multinational Cyber Defense Education and Training* (MN CD E&T) de la OTAN. El objetivo del proyecto era crear una plataforma de coordinación para la enseñanza y capacitación en ciberdefensa y desarrollar nuevas iniciativas para contribuir al desarrollo de capacidades en el área y la interoperabilidad en la OTAN.

En 2017, Portugal se unió al Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN (CCDCOE), diseñado para mejorar el entrenamiento, la formación y la capacitación en el campo de la ciberdefensa. Y, en 2019, se instaló en el país la sede principal de la *Communications and Information Academy* (Academia NCI), que reúne todas las actividades asociadas a la educación y la capacitación impartidas por la Agencia, especialmente las relacionadas con el ciberespacio.

Portugal también participa en ejercicios como el *Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise* (CWIX), un ejercicio anual para mejorar la interoperabilidad entre los miembros de la Alianza y las naciones asociadas, y la Coalición Cibernética, uno de los ejercicios de ciberdefensa más grandes del mundo.

5 CONCLUSIÓN

A lo largo de este artículo es posible constatar la creciente expansión que el sector cibernético ha logrado en la organización de la defensa portuguesa. Aunque los documentos rectores de la planificación estratégica del país se remontan a 2014 y requieren una actualización, parece que en ese momento se consideraron acciones, tanto defensivas como ofensivas, en este campo para garantizar los intereses nacionales.

Además, la propuesta ya aprobada que guiará la elaboración de un nuevo CEDN, en que el ciberespacio cobró más protagonismo, tal como las LPM de 2019 y 2023, en las cuales el sector recibió mayor asignación presupuestaria, sumadas a las iniciativas para la producción de documentos estratégicos específicos y las reformas organizativas, con énfasis en la creación del COCiber, son importantes indicadores de que el dominio cibernético ha ganado protagonismo estratégico en las operaciones presentes y futuras.

En el contexto en el que las Fuerzas Armadas deben estar preparadas para actuar de manera interoperable y en múltiples dominios, el intercambio de entrenamiento, ejercicios y datos, así como la capacitación y retención de personal cualificado, sumadas a las inversiones en tecnologías de vanguardia son los elementos indispensables para la planificación estratégica en defensa. En este ámbito, la capacidad cibernética es un instrumento crucial en tiempos de guerra y paz para la seguridad y la prosperidad de los países.

Por tanto, Portugal ha dado, sin duda, pasos cruciales en los últimos años en el refuerzo de su ciberdefensa, aunque aún debe superar importantes obstáculos, como la no ejecución de la inversión prevista en 2022 para formar el Centro de Ciberdefensa, que no sigue estando por debajo de lo necesario en términos cualitativos y cuantitativos, y el importante retraso en la creación de la Escuela de Ciberdefensa. Estos hechos aumentan las expectativas para el ciclo de planificación estratégica de defensa recién iniciado.

REFERENCIAS

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. Disponible en: https://www.idn.gov.pt/pt/noticias/Paginas/Ciclo-de-Revis%C3%A3o-do-Conceito-Estrat%C3%A9gico-de-Defesa-Nacional.aspx. Acceso en: 23 oct. 2024.

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

DAEHNHARDT, P. A Resposta da NATO à Nova Ordem Euro-Atlântica Confrontacional. **IDNBrief**, [*s.l.*], p. 1-2, 2022. Disponibleen: https://run.unl.pt/handle/10362/167738?mode=full. Acceso en: 23 oct. 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. Disponible en: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Acceso en: nov. 2024.

GASPAR, C. O Conceito Estratégico de Madrid. **IDN Brief**, [*s. l.*], 2022. Disponible en: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Acceso en: 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. Disponible en: https://www.dn.pt/edicao-do-dia/01-mai-2023/ciberdefesa-volta-a-estaca-zero-emgfa-vai-agora-abrir-concurso-publico-internacional-16262021.html/ Acceso en: agto. 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. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_112964.htm Acceso en: agto, 2024.

OTAN - Organização do Tratado do Atlântico Norte. Strategic Concept. **NATO Summit**, Madrid, 2022. Disponible en: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf. Acceso en: agto. 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. Disponible en: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf. Acceso en: jun. 2023

PORTUGAL. **Resolução do Conselho de Ministros n. 26/2013 de 11 de abril**. Defesa 2020. Lisboa: Ministério da Defesa Nacional, 2013b. Disponible en: https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Defesa-2020.pdf. Acceso en: agto. 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. Disponible en: https://diariodarepublica.pt/dr/detalhe/despacho/13692-2013-3295679. Acceso en: agto. 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. Disponible en: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/36-2015-67468089. Acceso en: agto. 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. Disponible en: https://diariodarepublica.pt/dr/detalhe/despacho/2536-2020-129529718. Acceso en: agto. 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. Disponible en: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924. Acceso en: agto. 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. Disponible en: https://diariodarepublica.pt/dr/detalhe/decreto-lei/19-2022-178080766. Acceso en: agto. 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. Disponible en: https://diariodarepublica.pt/dr/detalhe/decreto-lei/34-2023-213345452. Acceso en: agto. 2024.

PORTUGAL. **O Centro de Ciberdefesa**, s.d. Disponible en: https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro. Acceso en: agto. 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. Disponible en: https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN%20brief%20julho_2022_2_TextoIntegral.pdf. Acceso en: 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. Disponible en: http://www.ebrevistas.eb.mil.br/CEEExAE/article/view/8496. Acceso en: 24 oct. 2024.

SERRA, M. Até ao fim do ano, Portugal vai quadruplicar os efetivos militares dedicados à ciberdefesa. **TSF Rádio Notícias**, Lisboa, abr. 2019. Disponible en: https://www.tsf.pt/politica/ate-ao-fim-do-ano-portugal-vai-quadruplicar-os-efetivos-militares-dedicados-a-ciberdefesa-10756302.html. Acceso en: 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. Disponible en: https://www.enabed2022.abedef.org/resources/anais/19/enabed2022/1658704156_ARQUIVO_c9ff3811d4843661952302187444486f8.pdf. Acceso en: agto. 2024.