INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2019/2020

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

A EDIFICAÇÃO DA CAPACIDADE DE CIBERDEFESA NACIONAL

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS E DA GUARDA NACIONAL REPUBLICANA.

Paulo Fernando Viegas Nunes

Coronel de Transmissões

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A EDIFICAÇÃO DA CAPACIDADE DE CIBERDEFESA NACIONAL

COR TM Paulo Fernando Viegas Nunes

Trabalho de Investigação Individual do CPOG 2019/2020

Pedrouços 2020

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A EDIFICAÇÃO DA CAPACIDADE DE CIBERDEFESA NACIONAL

COR TM Paulo Fernando Viegas Nunes

Trabalho de Investigação Individual do CPOG 2019/2020

Orientador: CALM António Gameiro Marques

Pedrouços 2020

Declaração de compromisso Antiplágio

Eu, **Paulo Fernando Viegas Nunes**, declaro por minha honra que o documento intitulado "**A edificação da capacidade de ciberdefesa nacional**" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **CPOG 2019/20** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 09** de **junho** de **2020**

Nunes Paulo
Digitally signed by Nunes Paulo
Date: 2019.12.17 21:27:53 +01'00'

Paulo Fernando Viegas Nunes

COR TM

Agradecimentos

A elaboração deste trabalho de investigação, abordando um tema transversal, em constante evolução doutrinária e tecnológica, constituiu um desafio tão gratificante como exigente, beneficiando de um conjunto de prestimosos contributos, que importa aqui salientar.

As minhas primeiras palavras, de agradecimento e elevado apreço, dirigem-se ao meu orientador, Contra-Almirante António Gameiro Marques, pelo saber partilhado, permanente disponibilidade, rigor e amizade, sempre reiterados. O seu profundo conhecimento, integrador das dinâmicas associadas à cibersegurança e ciberdefesa nacional, constituíram uma motivação adicional para pensar "fora da caixa" e para ousar abrir novos caminhos ao longo deste trabalho.

A todos os que com a sua visão e experiência muito contribuíram para a construção de um quadro de análise mais consistente e realista. Neste âmbito, salienta-se a gratificante troca de ideias com muitos dos responsáveis pela operacionalização da estratégia nacional de segurança no ciberespaço como Lino Santos, Capitão-de-Mar-e-Guerra Hélder Fialho de Jesus, Carlos Cabreiro, Rogério Bravo e representantes dos Serviços de Informações de Segurança.

Pela disponibilidade demonstrada e visão enquadradora, apoiando a reflexão e debate dos tópicos estruturantes deste trabalho, foi importante poder contar com os contributos do Vice-Almirante Silvestre Correia, Tenente-General Martins Pereira, Major-General Xavier de Sousa, Major-General Maia Pereira, Major-General (Reserva) Passos Morgado, Brigadeiro-General Bento Soares, Comodoro Bento Domingues e Brigadeiro-General João Rocha.

Aos auditores do terceiro Curso de Planeamento de Operações no Ciberespaço do Instituto Universitário Militar, em especial ao Diretor do Curso Tenente-Coronel José Brito Sousa, pelo pronto apoio e disponibilidade demonstradas na operacionalização da resposta ao questionário e na organização do *focus group* realizado no âmbito desta investigação.

Uma referência especial é também devida ao Coronel Mário Álvares pela sua permanente disponibilidade e apoio, instrumentais para o tratamento dos dados e estruturação deste estudo.

Aos auditores do Curso de Promoção a Oficial General 2019/2020, pelo ambiente de saudável convívio e camaradagem, debate de ideias e gratificante partilha de conhecimento, que em muito facilitaram a conclusão do presente trabalho de investigação.

Um agradecimento muito especial à minha família, pelo apoio incondicional, paciência e inspiração que constituíram o meu "Norte" ao longo desta viagem.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

Fruto da revolução digital, as modernas sociedades tornaram-se dependentes da internet e do ciberespaço, levantando novos riscos à Segurança e Defesa Nacional. De forma a cumprir a sua missão, as Forças Armadas já assumiram o ciberespaço como um domínio de operações, a par do mar, terra e ar.

Propondo a definição de uma Estratégia Militar para o Ciberespaço, alinhada com a Estratégia Nacional de Segurança do Ciberespaço, este estudo analisa os desafios associados ao desenvolvimento da capacidade de ciberdefesa das Forças Armadas. Para esse efeito, utilizou-se um raciocínio dedutivo, alicerçado numa estratégia de investigação qualitativa, no estudo de caso, na análise documental e nos dados recolhidos a partir de um questionário e de entrevistas realizadas a especialistas ligados à cibersegurança e ciberdefesa nacional.

Dos resultados obtidos, concluiu-se que a dinamização da edificação da capacidade de ciberdefesa nacional, passa pela materialização de uma Estratégia Militar para o Ciberespaço, coerente, sinérgica e articulada nas suas dimensões operacional, estrutural e genética.

Este processo de transformação, assente numa nova visão estratégica e num plano de desenvolvimento da capacidade de ciberdefesa, permitirá às Forças Armadas defender as suas redes contra ciberataques e realizar operações militares no ciberespaço, contribuindo desta forma para assegurar a ciberdefesa nacional.

Palavras-chave: Ciberespaço, Cibersegurança, Ciberdefesa, Estratégia Militar para o Ciberespaço, Desenvolvimento da capacidade de ciberdefesa nacional.

Abstract

Driven by the digital revolution, modern societies became internet and cyberspace dependent, raising new risks to national security and defence. In order to fulfil its mission, the Armed Forces already incorporated cyberspace as a new domain of operations, side by side with land, sea and air.

Proposing the definition of a cyberspace military strategy, aligned with the national cyberspace security strategy, this study conducts an analysis of the main challenges raised by the Armed Forces cyber defence capability development process. With this aim, it was used a deductive reasoning, supported by a qualitative research strategy, a case study approach, documental analysis and data collected from a questionnaire and an interview addressed to cybersecurity and cyber defence experts.

From the results achieved, it was possible to conclude that the enhancement of the national cyber defence capability building process, requires the adoption of a national cyberspace military strategy, coherent, synergetic and articulated along its operational, structural and genetic dimensions.

This transformational process, supported by a strategic vision and a cyber defence capability development plan, will allow the Armed Forces to defend their networks against cyberattacks and to conduct military operations in cyberspace, therefore assuring the national cyber defence.

Keywords: Cyberspace, Cyber Security, Cyberspace Military Strategy, National Cyber Defence Capability Development.

Lista de abreviaturas, siglas e acrónimos

A	Ameaças
ACO	*Allied Command Operations* (Comando Aliado para as Operações)
AJP	*Allied Joint Publication* (Publicação Aliada Conjunta)
BTID	Base Tecnológica e Industrial de Defesa
C2	Comando e Controlo
CAIH	*Cyber Academia and Innovation Hub Project* (Projeto integrador de inovação e do meio académico na área do ciberespaço)
CCD	Centro de Ciberdefesa das Forças Armadas
CCDCOE	*Cooperative Cyber Defence Centre of Excellence* (Centro de Excelência Cooperativo em Ciberdefesa)
CCDFFAA	Capacidade de Ciberdefesa das Forças Armadas
CCDN	Capacidade de Ciberdefesa Nacional
CDP	*Capability Development Plan* (Plano de Desenvolvimento de Capacidades)
CDM	*Capability Development Mechanism* (Mecanismo de Desenvolvimento de Capacidades)
CEDN	Conceito Estratégico de Defesa Nacional
CEM	Conceito Estratégico Militar
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CERT	*Computer Emergency Response Team* (Equipa de Resposta a Emergências Computacionais/Informáticas)
CIRC	*Computer Incident Response Capability* (Capacidade de Resposta a Incidentes em Computadores)
CISMIL	Centro de Informações e Segurança Militar
CMCD	Comité de Monitorização da Ciberdefesa
CNCS	Centro Nacional de Cibersegurança
CNO	*Computer Network Operations* (Operações em Redes de Computadores)
CO	Comando Operacional
COCIBER	Comando de Operações no Ciberespaço
CONOPS	Conceito de Operações
COPD	*Comprehensive Operations Planning Directive* (Diretiva para o Planeamento Integrado de Operações)

CPDM	Ciclo de Planeamento de Defesa Militar
CPOCIBER	Curso de Planeamento de Operações no Ciberespaço
CSDC	Conselho Superior de Defesa do Ciberespaço
CSDN	Conselho Superior de Defesa Nacional
CSI	Comunicações e Sistemas de Informação
CSIRT	*Computer Security Incidents Response Team* (Equipa de Resposta a Incidentes de Segurança Computacional/informática)
CSSC	Conselho Superior para a Segurança do Ciberespaço
CWIX	*Coalition Warrior Interoperability, eXploration, eXperimentation, eXamination eXercise* (Exercício de Interoperabilidade de Forças NATO)
CyOC	*Cyberspace Operations Center* (Centro de Operações para o Ciberespaço)
DEEMGFA	Diretiva Estratégica do Estado-Maior-General das Forças Armadas
DF	Diretor Funcional
DGRDN	Direção-Geral de Recursos da Defesa Nacional
DIRCSI	Direção de Comunicações e Sistemas de Informação
DMPDM	Diretiva Ministerial de Planeamento de Defesa Militar
DN	Defesa Nacional
DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade
EMCIBER	Estratégia Militar para o Ciberespaço
EME	Estado-Maior do Exército
EMGFA	Estado-Maior-General das Forças Armadas
ENCD	Estratégia Nacional de Ciberdefesa
ENSC	Estratégia Nacional de Segurança no Ciberespaço
EUA	Estados Unidos da América
FED	Fundo Europeu de Defesa
FFAA	Forças Armadas
FND	Forças e elementos Nacionais Destacados
G4	Grupo dos Quatro (Centro Nacional de Cibersegurança, Centro de Ciberdefesa, Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica e Serviços de Informações de Segurança)
H	Hipótese
IDN	Instituto da Defesa Nacional

ID&I	Investigação, Desenvolvimento e Inovação
ISR	*Intelligence, Surveillance and Reconnaissance* (Informações, Vigilância e Reconhecimento)
IUM	Instituto Universitário Militar
LA	Linha de Ação
LE	Linha Estruturante
LO	Linha Orientadora
LOENCD	Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa
LPM	Lei de Programação Militar
MDN	Ministro da Defesa Nacional
MNCDE&T	*Multinational Cyber Defence Education and Training Project* (Projeto Multinacional de Educação e Treino em Ciberdefesa)
NAC	*North Atlantic Council* (Conselho do Atlântico Norte)
NATO	*North Atlantic Treaty Organization* (Organização do Tratado do Atlântico Norte)
NCI Academy	*NATO Communications and Information Academy* (Academia de Comunicações e Informação da NATO)
NCIRC	*NATO Computer Incident Response Capability* (Capacidade de Resposta a Incidentes em Computadores da NATO)
NCRP	*NATO Crisis Response Process* (Processo de Resposta a Crises da NATO)
O	Oportunidades
OE	Objetivo Específico
OEE	Objetivo Estratégico Estruturante
OG	Objetivo Geral
OpCiber	Operações no Ciberespaço
P	Potencialidades
PDC	Processo de Desenvolvimento de Capacidades
PDCCD	Plano de Desenvolvimento da Capacidade de Ciberdefesa
PESCO	*PErmanent Structured Cooperation* (Cooperação Estruturada Permanente)
Q	Questão
QC	Questão Central
QD	Questão Derivada
RCM	Resolução do Conselho de Ministros
RE	Requisitos Estratégicos

RH	Recursos Humanos
RO	Requisitos Operacionais
SCEPVA	*Sovereign Cyber Effects Provided Voluntarily by Allies* (Efeitos Soberanos no Ciberespaço Produzidos Voluntariamente por Aliados).
SDN	Segurança e Defesa Nacional
SIC	Sistemas de Informação e Comunicação
SIS	Serviços de Informações de Segurança
SWOT	*Strengths, Weaknesses, Opportunities and Threats* (Forças, Fraquezas, Oportunidades e Ameaças)
TII	Trabalho de Investigação Individual
U	Utilizadores
UE	União Europeia
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
V	Vulnerabilidades

1. Introdução

O desenvolvimento tecnológico e a transformação digital das sociedades conheceram um forte impulso ao longo das últimas décadas. A internet, produto deste processo, estreitou distâncias, criou redes, gerando uma interação à escala global, tanto no plano social, económico como militar.

Estruturado com base na internet, o ciberespaço apresenta potencialidades, mas também vulnerabilidades que podem ser exploradas por atores mal-intencionados. Novas ameaças, muitas vezes de natureza híbrida, são cada vez mais frequentes e complexas. Pelas vantagens oferecidas, os ciberataques lançados por atores hostis, geram novos riscos, comprometendo a Segurança e Defesa Nacional (SDN).

A atuação das Forças Armadas (FFAA) depende funcionalmente da disponibilidade e fiabilidade dos seus Sistemas de Informação e Comunicação (SIC). Atendendo à elevada sofisticação tecnológica dos modernos sistemas de armas, um ataque lançado através do ciberespaço pode ter um efeito disruptivo e/ou destrutivo, de natureza cinética e não cinética.

O ciberespaço, não pode assim ser considerado um domínio marginal aos assuntos militares, sendo de assinalar que, em 2016, na cimeira de Varsóvia, os chefes de estado e de governo da Aliança Atlântica assinaram um compromisso destinado a reforçar a sua defesa cibernética (*cyber defence pledge*) e assumiram formalmente o ciberespaço como um novo domínio das operações, a par da terra, mar e ar (*North Atlantic Treaty Organization* [NATO], 2016a). Na cimeira de Bruxelas (NATO, 2018a), identificaram também a ciberdefesa como uma das áreas prioritárias da defesa e dissuasão da Aliança, concordando com a possibilidade de a NATO poder vir a contar com capacidades cedidas voluntariamente por algumas nações para assegurar o cumprimento das suas operações no âmbito da ciberdefesa (NATO, 2018b).

Na recente cimeira em Londres, reforçando as conclusões da cimeira de Bruxelas, os Aliados anunciaram o aumento das suas ferramentas "para responder a ciberataques, fortalecer a sua capacidade de preparação, de dissuasão e defesa contra táticas híbridas que procuram minar a segurança e as sociedades" (NATO, 2019a).

Na sequência deste processo de reconhecimento formal e desenvolvimento de capacidades, várias nações aliadas, tal como Portugal, têm vindo a ser confrontadas com a necessidade de levantar Comandos e estruturas operacionais, especialmente dedicadas à proteção das suas redes e à condução de Operações no Ciberespaço (OpCiber).

As obrigações internacionais assumidas por Portugal ao nível da ciberdefesa, tanto no quadro NATO como da União Europeia (UE), impõem também novos requisitos ao nível operacional, estrutural e genético, a considerar na edificação da Capacidade de Ciberdefesa Nacional (CCDN).

Em linha com o prescrito na Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, publicada através da Resolução do Conselho de Ministros (RCM) n.º 92/2019, de 05 de junho, e atendendo à Diretiva Estratégica do Estado-Maior-General das Forças Armadas (DEEMGFA) de 2018-2021 (EMGFA, 2018), este trabalho assume especial acuidade e oportunidade.

O objeto do presente estudo, face ao enquadramento apresentado, é assim a edificação da CCDN.

Sem prejuízo da sua contextualização, este trabalho foi conduzido em linha com as delimitações de tempo, espaço e conteúdo (Santos & Lima, 2019, p.42), que a seguir se indicam.

Em termos temporais, o estudo é limitado à última década, estruturante do levantamento de capacidades nacionais e, prospectivamente, até 2025, horizonte temporal dos documentos de referência analisados.

Envolvendo esta investigação a definição de uma Estratégia Militar para o Ciberespaço (EMCIBER), na recolha de dados segundo o método de entrevista, utilizou-se uma amostra representativa dos decisores que influenciam o desenvolvimento da CCDN e/ou a cibersegurança do Estado.

Ao nível do conteúdo, abordam-se essencialmente as implicações do tema ao nível da EMCIBER. O seu impacto nas restantes áreas da estratégia militar será abordado apenas de forma complementar, por não constituir o foco primário deste trabalho.

Face ao exposto, o Objetivo Geral (OG) e os Objetivos Específicos (OE) formulados são apresentados no Quadro 1.

Quadro 1 – Objetivos da investigação

Objetivo Geral
Avaliar o processo de desenvolvimento da capacidade de ciberdefesa das FFAA, de forma a dinamizar a edificação da CCDN, e a dotar as FFAA com uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço.
Objetivos Específicos
OE 1: Propor, face ao impacto estratégico do ambiente da informação, a definição de uma EMCIBER.
OE 2: Analisar, ao nível da estratégia operacional, o impacto do reconhecimento nacional do ciberespaço como quarto domínio das operações.
OE 3: Analisar os constrangimentos dos recursos humanos das FFAA (EMGFA e Ramos) e os diferentes modelos orgânicos existentes, de forma a promover o levantamento da estrutura de ciberdefesa das FFAA (estratégia estrutural).
OE 4: Analisar o modelo de desenvolvimento da capacidade de ciberdefesa das FFAA (estratégica genética).

Em linha com os objetivos elencados, foi definida a seguinte Questão Central (QC): *Qual o modelo a adotar para a edificação da Capacidade de Ciberdefesa das FFAA (CCDFFAA), de forma a dinamizar a edificação da CCDN, dotando as FFAA com uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço?*

O estudo, para além da presente introdução (primeiro capítulo), estrutura-se em cinco capítulos a que acrescem as conclusões. O segundo, apresenta a revisão da literatura, a metodologia e o método. O terceiro, analisa o impacto estratégico do ciberespaço e propõe a definição da EMCIBER. Este capítulo, faz a ponte com os seguintes, onde se caracterizam as componentes operacional (capítulo quarto), estrutural (capítulo quinto) e genética (capítulo sexto) desta estratégia. Nas conclusões, sintetizam-se o procedimento metodológico e os resultados obtidos, demonstrando a forma como será possível dinamizar a edificação da CCDN. Como corolário deste trabalho, apresentam-se recomendações e sugestões para investigações futuras.

2. Enquadramento teórico, metodologia e método

O tema deste Trabalho de Investigação Individual (TII) enquadra-se no âmbito das Ciências Militares, no domínio do "Estudo das Crises e Conflitos Armados" – subáreas "Estratégia Militar" e "Planeamento Estratégico Militar"; e das "Técnicas e Tecnologias Militares" – subáreas de "Ciberdefesa/Cibersegurança" e "Estudos de Componente" (Centro de Investigação e Desenvolvimento do Instituto Universitário Militar, 2018).

2.1. Estado da arte e modelo de análise

O estado da arte, incluindo os fundamentos teóricos aqui referidos, enformou a realização deste trabalho.

2.1.1. Conceptualização estratégica do ciberespaço

De acordo com Couto (1988, p.214-215), cabe à política a definição dos interesses nacionais e a sua prossecução, procurando satisfazer os objetivos teleológicos do Estado, ou seja, o progresso, bem-estar e segurança. Face a ações contrárias à satisfação dos seus interesses, o Estado pode ter que impor a sua vontade de forma violenta. Segundo Clausewitz (1976), o conflito é visto como uma consequência da condução da política por outros meios, dando lugar à definição de uma estratégia.

Reconhecendo que a estratégia do Estado é una na sua conceção, unificando de forma coerente todo o sistema estratégico, Beaufre (1965) define, ao nível político-estratégico, uma "estratégia total", agrupando todos os instrumentos de coação em estratégias gerais, diferenciadas quanto aos seus campos de aplicação: interno (político), externo (diplomático), psicológico (ambiente da informação), económico e militar. Segundo este autor, cada estratégia geral decompõe-se em estratégias particulares, diferenciáveis nos instrumentos, cenários e formas de emprego dos meios, procurando atingir fins específicos. À luz deste referencial teórico, validado por Couto (1988, p.227), a definição de qualquer estratégia deve clarificar não só o seu âmbito (domínio da ação) como também a sua finalidade (consequências a produzir).

Nos vários domínios da estratégia, "situa-se a charneira entre a conceção e a execução das ações estratégicas, isto é, entre o que se pretende ou deve fazer e o que os meios possibilitam" (Alves, 1998, p.121). Assim, como elementos distintos e essenciais para a materialização da estratégia, importa distinguir os seus "aspetos operacionais (ligados à utilização dos meios), genéticos (associados à geração e sustentação de meios) e os aspetos estruturais (correspondentes à composição, organização ou articulação dos meios)" (Couto, 1988, p.230).

De acordo com este autor, a estratégia operacional trata da conceção e execução da manobra estratégica (conceito de emprego/operações), refletindo a aplicação de uma doutrina específica

para aplicação dos meios (maturidade doutrinária). Relativamente à estratégia estrutural, esta tem por objetivo a "criação de novas estruturas, que conduzam à eliminação ou atenuação das vulnerabilidades, a um reforço das potencialidades e, em última análise a um melhor rendimento dos meios e recursos" (Couto, 1988, p.232), consubstanciando-se essencialmente através de duas vertentes: estruturas orgânicas e integração das capacidades operacionais. Finalmente, no que toca à estratégia genética, esta define-se através de um processo de desenvolvimento de capacidades, explorando sinergias e a cooperação internacional, sempre que ajustado.

Com base na missão atribuída às FFAA pela Constituição da República Portuguesa, Resolução da Assembleia da República n.º 15/2005, de 07 de abril, alinhada com o Conceito Estratégico de Defesa Nacional (CEDN), RCM n.º 19/2013, de 21 de março, a estratégia militar é responsável pela aplicação da coação militar e articula-se através das suas estratégias particulares (terrestre, naval e aeroespacial), envolvendo para esse efeito cada um dos Ramos. O reconhecimento do ciberespaço, como novo domínio das operações, faz assim surgir uma nova estratégia particular: a EMCIBER.

A definição desta estratégia, nas suas vertentes operacional, estrutural e genética, enquadra a edificação da CCDFFAA, destinada a garantir a defesa dos SIC militares e a condução de OpCiber. A CCDN decorre da CCDFFA e da sua articulação com a cibersegurança nacional.

2.1.2. Ciberespaço e ambiente da informação

A utilização do ciberespaço e do ambiente da informação assume hoje um caráter transversal e multidisciplinar, sendo evidente o seu contributo para a definição dos diversos tipos de forças (tangíveis e intangíveis) de uma unidade política.

Segundo uma perspetiva operacional, a NATO entende o ciberespaço como "o domínio virtual, de natureza global e comum, dentro do ambiente da informação, composto pelos sistemas de comunicação, informação e outros sistemas de natureza eletrónica, incluindo a sua interação e a informação, de natureza digital, que é armazenada, processada e transmitida através desses sistemas" (NATO, 2018c, p.A-1). Em termos nacionais, conforme refere o ponto primeiro da ENSC, este é também entendido como "um ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

O ambiente da informação assume uma importância crescente, fruto das dinâmicas de poder geradas no ciberespaço e a partir dele. Importa assim reconhecer o carácter dual da informação, como recurso, no contexto dos processos de decisão, e/ou, como vetor de ataque, enquanto instrumento de exercício do poder. Na Figura 1, a designada "pirâmide cognitiva", construída a partir dos seus quatro níveis de abstração (dados, informação, conhecimento e

sabedoria), reflete a natureza dos efeitos produzidos (físicos, de sintaxe/lógicos e semânticos/cognitivos) e os diversos domínios onde os mesmos são aplicados.

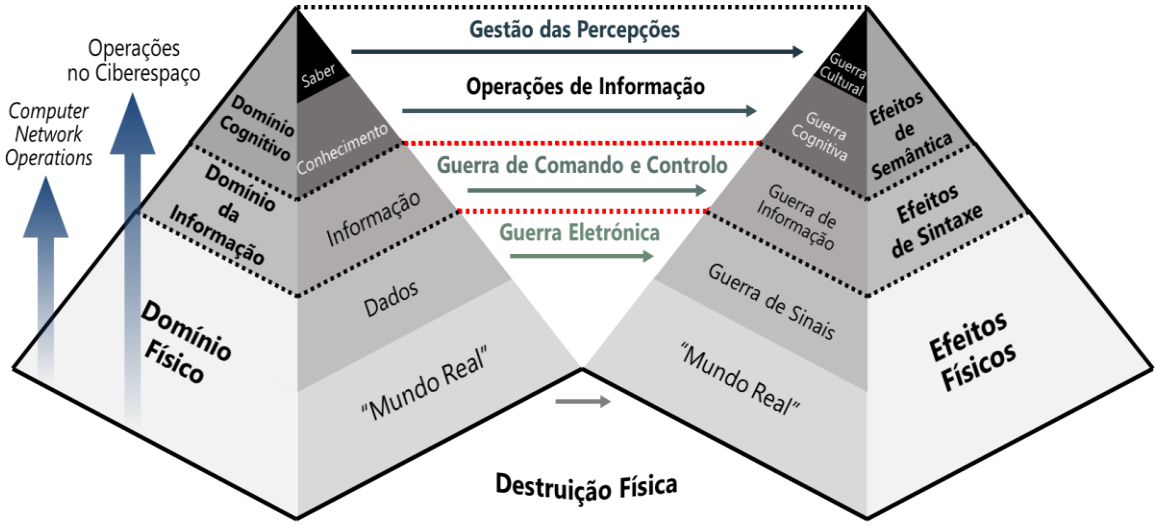


Figura 1 – "Pirâmide cognitiva" e utilização operacional do ciberespaço

Face à doutrina existente, as FFAA atuam de forma articulada no domínio: físico – destruição física e guerra eletrónica/guerra de sinais; da informação – guerra de Comando e Controlo (C2)/guerra de informação; e, cognitivo – operações de informação/guerra cognitiva e/ou gestão das perceções.

Relativamente às OpCiber, verifica-se que o seu enquadramento doutrinário, ainda em consolidação, é indissociável do ambiente da informação. Desta forma, as *Computer Network Operations* (CNO), de natureza iminentemente tática, produzem efeitos físicos e de sintaxe/lógica. As OpCiber (*Allied Joint Publication* [AJP]-3.20, 2020), conduzidas ao nível operacional, sem prejuízo de utilizarem efeitos físicos (*e.g.*, negar o acesso ou exfiltrar informação do oponente), podem atingir efeitos de sintaxe e de semântica. Finalmente, as operações de informação (AJP-3.10, 2009), assumindo um papel de coordenação, planeiam essencialmente efeitos no domínio cognitivo, ao nível operacional/estratégico.

Reconhecendo que o ciberespaço constitui um domínio global, dentro do ambiente da informação, na taxonomia relativa às OpCiber (AJP-3.20, 2020), a NATO refere que estas podem ser de natureza defensiva ou ofensiva. Estes dois tipos de operações, caracterizadas no Apêndice A, materializam-se no e através do ciberespaço, para salvaguardar a liberdade de ação das forças amigas e/ou para atingir objetivos operacionais.

2.1.3. Modelo de análise

Esta investigação desenvolve-se em conformidade com o modelo de análise apresentado no Quadro 2.

Quadro 2 – Modelo de análise

Objetivo Geral (OG)	Avaliar o processo de desenvolvimento da capacidade de ciberdefesa das FFAA, de forma a dinamizar a edificação da capacidade de ciberdefesa nacional, e a dotar as FFAA com uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço.					
Objetivos Específicos	**Questão Central**	Qual o modelo a adotar para a edificação da capacidade de ciberdefesa das FFAA, de forma a dinamizar a edificação da capacidade de ciberdefesa nacional, e a dotar as FFAA com uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço?				
	Questões Derivadas (QD)	**Hipóteses (H)**	**Conceitos/ constructos**	**Dimensões/ variáveis**	**Indicadores** Questões (Q) da Entrevista	**Técnicas de recolha de dados**
OE1 Propor, face ao impacto estratégico do ambiente da informação, a definição de uma estratégia militar para o ciberespaço.	**QD1** Quais as componentes que, face ao impacto estratégico do ambiente da informação, deverão fazer parte da definição de uma estratégia militar para o ciberespaço?	**H1** O impacto estratégico do ambiente da informação obriga à criação da estratégia militar para o ciberespaço (componentes operacional, estrutural e genética), sendo necessário definir o seu âmbito e finalidade.	Estratégia militar para o ciberespaço	Âmbito	Q1A	Entrevista Revisão bibliográfica
				Finalidade	Q1B	
OE2 Analisar, ao nível da estratégia operacional, o impacto do reconhecimento nacional do ciberespaço como quarto domínio operacional.	**QD2** Qual é, ao nível da estratégia operacional, o impacto do reconhecimento nacional do ciberespaço como quarto domínio operacional?	**H2** A atuação das FFAA no ciberespaço exige a existência de doutrina específica e de um conceito de emprego de forças/conceito de operações.	Estratégia operacional para o ciberespaço	Conceito de operações	Q2, Q7A, Q7B	Entrevista Revisão bibliográfica
				Maturidade doutrinária	Q3, Q7A, Q7B	Entrevista Questionário
OE3 Analisar os constrangimentos dos recursos humanos das FFAA e os diferentes modelos orgânicos existentes, de forma a promover o levantamento da estrutura nacional de ciberdefesa (estratégia estrutural).	**QD3** De que forma se pode, atendendo aos constrangimentos dos recursos humanos das FFAA e aos diferentes modelos orgânicos existentes, promover o levantamento da estrutura nacional de ciberdefesa (estratégia estrutural)?	**H3** O modelo orgânico da estrutura nacional de ciberdefesa, inserindo-se na estrutura das FFAA, deverá articular-se com a estrutura nacional de cibersegurança.	Estratégia estrutural para o ciberespaço	Estrutura organizacional	Q4	Entrevista Revisão bibliográfica
				Integração de capacidades operacionais	Q5	Entrevista Questionário
OE4 Analisar o modelo de desenvolvimento da capacidade de ciberdefesa das FFAA (estratégica genética).	**QD4** Qual o modelo de desenvolvimento da capacidade de ciberdefesa das FFAA a adotar (estratégica genética)?	**H4** A edificação da capacidade de ciberdefesa das FFAA deverá estar alinhada com o ciclo de desenvolvimento de capacidades nacional, NATO e da UE, de forma a explorar sinergias e a potenciar a cooperação internacional.	Estratégia genética para o ciberespaço	Processo de desenvolvimento da capacidade	Q6	Entrevista Revisão bibliográfica
				Sinergias nacionais	Q7A	
				Cooperação internacional	Q7B	

Na construção deste modelo, utilizaram-se os princípios e ferramentas da conceptualização estratégica para analisar, propor e avaliar. A edificação da CCDN é também equacionada neste contexto (Figura 2).

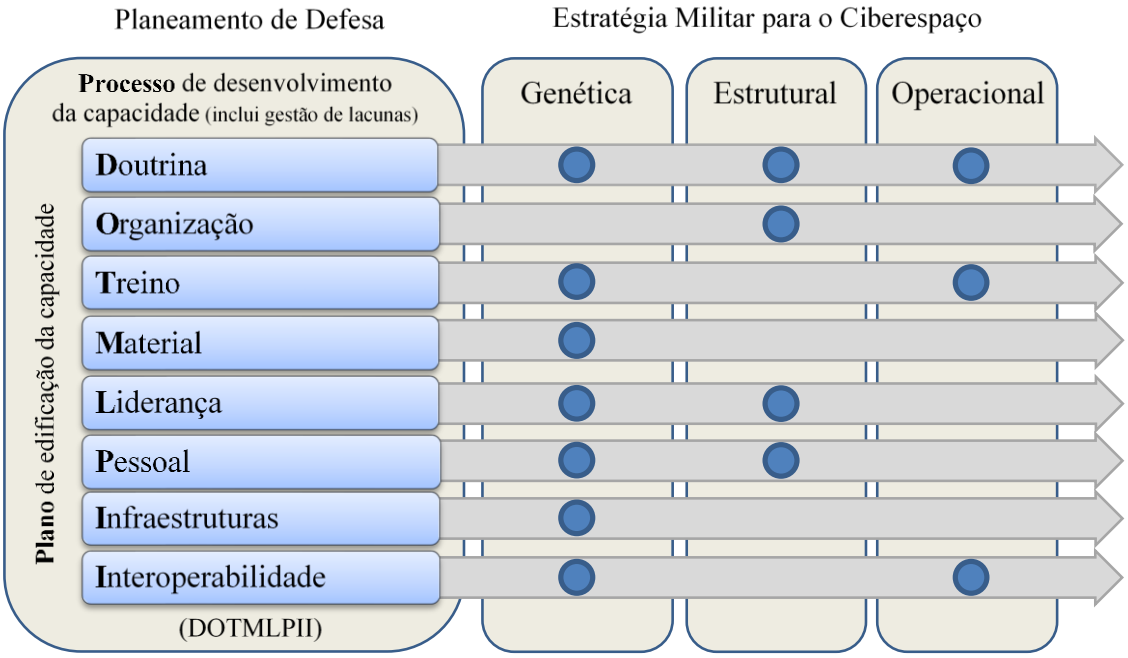


Figura 2 – Modelo de desenvolvimento da CCDN

Fonte: Adaptado a partir de EMGFA (2019b).

2.2. Metodologia e método

2.2.1. Metodologia

O percurso metodológico estrutura as fases: exploratória, incluindo a revisão da literatura e o procedimento metodológico (Quivy & Campenhoudt, 2003); analítica, envolvendo a recolha de dados e análise dos resultados; e conclusiva, orientada para a sua avaliação e discussão.

Metodologicamente, esta investigação seguiu um raciocínio de natureza hipotético-dedutiva (Freixo, 2011), testando teorias e utilizando a experiência para, a partir daí, construir/reformular o quadro teórico de referência, explorando uma estratégia essencialmente qualitativa e um desenho de pesquisa de tipo estudo de caso.

2.2.2. Método, participantes e procedimento

O procedimento metodológico para a recolha de informação concretizou-se em várias etapas, conforme se ilustra na Figura 3.

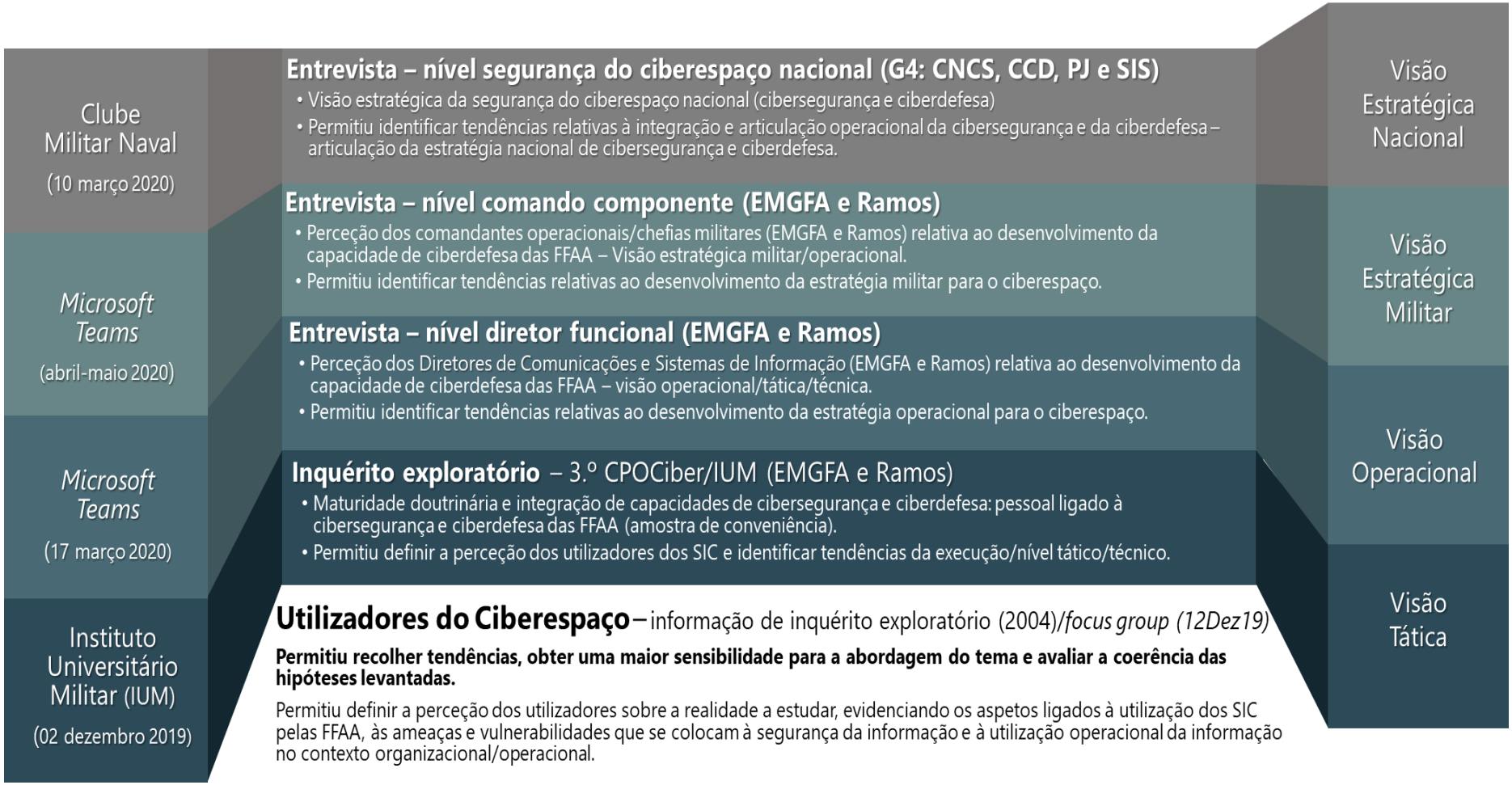


Figura 3 – Técnicas de recolha de dados e resultados obtidos

A primeira fase, incluiu a análise da informação recolhida numa investigação anterior, afim ao tema de estudo (Nunes, 2004), tendo a mesma sido atualizada e validada. Para esse efeito, foi utilizado um *focus group*, envolvendo 21 auditores do terceiro Curso de Planeamento de Operações no Ciberespaço (3.º CPOCIBER) do Instituto Universitário Militar (IUM), considerados uma amostra empírica (Bryman, 2012, pp.201-203) válida. As conclusões do *focus group*, encontram-se sintetizadas no Apêndice B. Adicionalmente, aplicou-se um questionário a esta amostra com duas perguntas de escolha múltipla de avaliação (Santos & Lima, 2019, p.79), cuja análise estatística é apresentada no Apêndice C.

A segunda fase, envolveu uma entrevista realizada a uma amostra representativa dos decisores ligados ao desenvolvimento da CCDFFAA ou que, assumindo responsabilidades na área da cibersegurança nacional, influenciam a edificação da CCDN. Foram entrevistadas, presencialmente e por correio eletrónico, 12 personalidades de mérito reconhecido, sendo oito militares e quatro civis, conforme Apêndice D. Utilizou-se uma entrevista semiestruturada, constituída por oito perguntas, realizada no período entre 12 de março e 30 de maio de 2020. Duas das questões formuladas foram objeto de tratamento estatístico (Apêndice C).

Numa última fase, os dados recolhidos a partir de relatórios e por observação do exercício de ciberdefesa "Ciber Perseu"[1] (Estado-Maior do Exército [EME], 2015; 2018), foram processados e utilizados no modelo de análise.

[1] Simula situações reais, desenvolvendo cenários e ferramentas de planeamento associadas ao objeto de estudo.

3. A estratégia militar para o ciberespaço

O ambiente internacional é hoje caracterizado como volátil, incerto, complexo e ambíguo, exigindo a articulação funcional das organizações em rede (McChrystal, 2015). Face às dinâmicas geradas e à sua contínua transformação, o ciberespaço condiciona profundamente o desenvolvimento das nações, gerando uma forte interdependência entre o mundo real e o ambiente virtual que o define.

Explorando a transversalidade de uma rede global, atores mal-intencionados como grupos ativistas, criminosos, ou terroristas, podem lançar ataques disruptivos e/ou destrutivos, contra indivíduos, organizações ou Estados. Na persecução dos seus interesses, as grandes potências mundiais também se desafiam e confrontam no ciberespaço.

Só um esforço coletivo dos Estados permitirá controlar este fenómeno e salvaguardar ao mundo digital o seu potencial virtuoso de transformação. Face ao espectro das novas ameaças, a evolução do ciberespaço não pode ser dissociada do desenvolvimento de novos processos de segurança, impondo a criação de uma Estratégia Nacional de Ciberdefesa (ENCD).

Atendendo a esta necessidade, pretende-se agora desenvolver um quadro de referência a partir do qual se propõe a definição de uma EMCIBER.

3.1. Enquadramento nacional

Portugal tem vindo ao longo dos últimos anos, a desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura do ciberespaço. Para esse efeito, estabelecendo um conjunto de prioridades estratégicas, o CEDN reconheceu a "informação e a segurança do ciberespaço" como um dos seus pilares estruturantes.

Refletindo esta orientação estratégica, no quadro da reforma "Defesa 2020", RCM n.º 26/2013, de 11 de abril, o Ministro da Defesa Nacional (MDN) determinou a criação de um Centro de Ciberdefesa (CCD) no âmbito do EMGFA e definiu a sua orientação política para a ciberdefesa (MDN, 2013), solicitando ao Chefe do Estado-Maior-General das Forças Armadas (CEMGFA) a apresentação de um Plano de Desenvolvimento da Capacidade de Ciberdefesa (PDCCD). Nesta sequência, conforme refletido na Figura 4, foi criado, em 2015, o CCD das FFAA.

Estes passos, foram também equacionados no quadro do levantamento de um Centro Nacional de Cibersegurança (CNCS), aprovado pelo Decreto-Lei n.º 69/2014, de 09 de maio, da revisão e atualização da ENSC, e da necessidade de dinamizar a edificação da CCDN (EMGFA, 2018). Neste âmbito, foram ainda considerados os esforços cooperativos já lançados por outros países e pelas organizações internacionais de que Portugal faz parte integrante (NATO e UE).

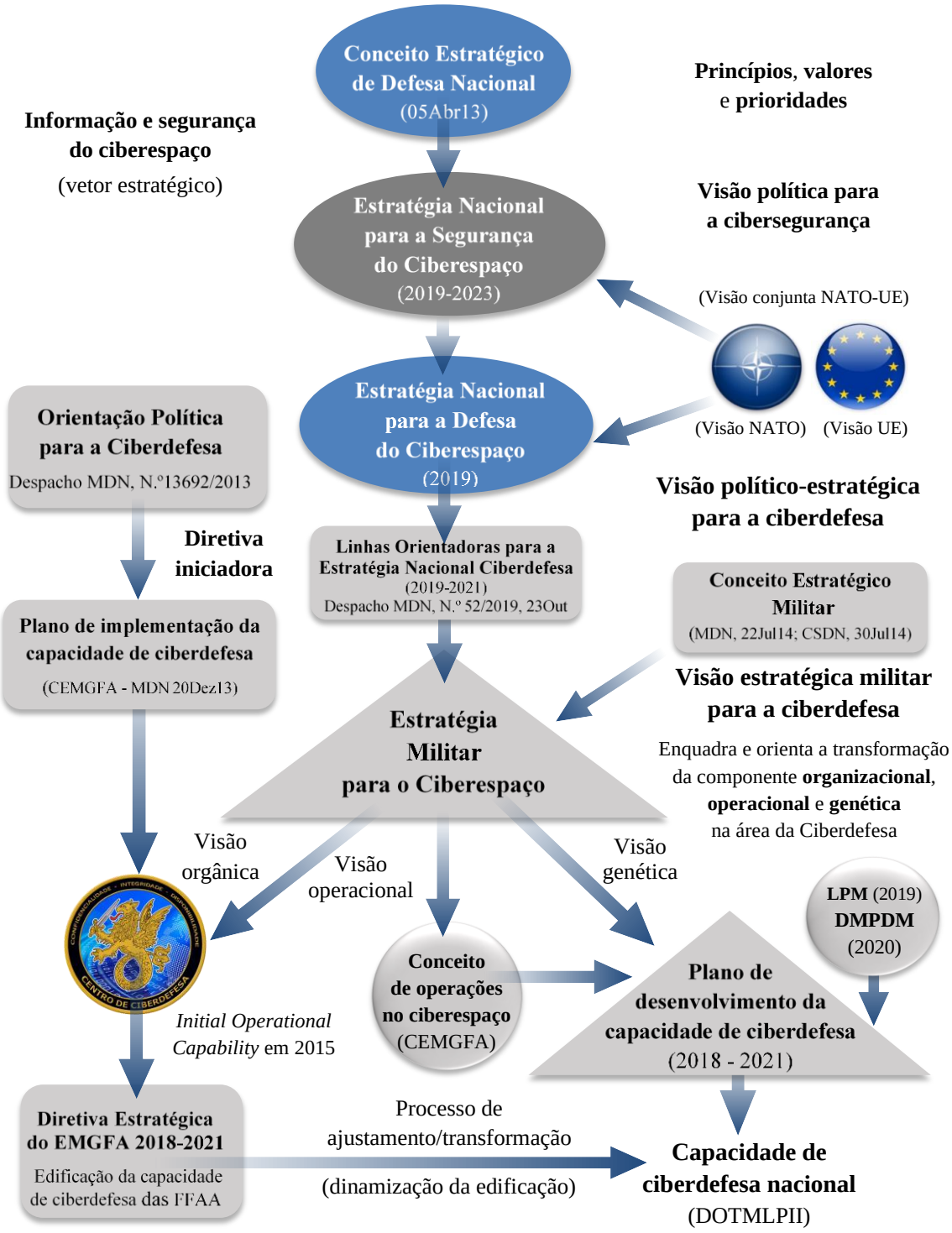


Figura 4 – Enquadramento conceptual da EMCIBER

Fonte: Adaptado a partir de Nunes (2018, p.94).

Constituindo o CNCS um órgão com responsabilidade de coordenação operacional, importa referir que, através da RCM n.º115/2017, de13 de julho, foi criado o Conselho Superior para a Segurança do Ciberespaço (CSSC), assumindo este órgão responsabilidades de coordenação estratégica da cibersegurança nacional, posteriormente consolidada através

do Art.º 5.º da Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço. A resposta a incidentes de cibersegurança decorre da atuação coordenada da rede nacional de *Computer Security Incident Response Teams* (CSIRT) e do designado Grupo dos Quatro (G4), composto pelo CNCS, CCD, Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica (UNC3T) e Serviços de Informações de Segurança (SIS).

No que se refere ao domínio da ciberdefesa, o Conceito Estratégico Militar (CEM) (Conselho Superior de Defesa Nacional [CSDN], 2014), ainda que de forma mitigada, incluiu a ciberdefesa nos cenários de emprego das FFAA, contemplando "a aplicação de medidas de segurança que garantam a salvaguarda da informação e a proteção das infraestruturas SIC das FFAA contra ciberataques, bem como, no caso de um ciberataque, a proteção e defesa das infraestruturas críticas nacionais e do governo eletrónico do Estado" (CSDN, 2014, p.19).

Tendo em vista o desenvolvimento de uma visão política para a ciberdefesa e a consequente criação de uma ENCD, por iniciativa ministerial, foram desenvolvidos diversos estudos (Nunes, 2018) e documentos de trabalho (MDN, 2019a; EMGFA, 2019a). Reforçando esta visão, através do seu Despacho n.º 52/2019, de 23 de outubro, o MDN aprovou as Linhas Orientadoras para a ENCD (LOENCD), determinando que "seja desenvolvida a ENCD e edificada a capacidade de condução de operações no, e através do, ciberespaço [...] de forma a garantir o alinhamento com a ENSC" (MDN, 2019b).

Sublinhando este alinhamento, o CEMGFA identificou, na sua DEEMGFA 2018-2021, a necessidade de atualizar o PDCCD e reforçar a edificação desta capacidade. A revisão da Lei de Programação Militar (LPM), aprovada pela Lei Orgânica n.º 02/2019, de 17 de junho, e a Diretiva Ministerial de Planeamento de Defesa Militar (DMPDM) do MDN (2020a), vieram também reforçar o seu caráter prioritário no planeamento de defesa militar.

Mais recentemente, o MDN (2020b) criou um Comité de Monitorização da Ciberdefesa (CMCD), na sua direta dependência, cuja missão é o acompanhamento permanente de todos os assuntos relacionados com a ciberdefesa nacional, garantindo assim a coerência e integração de esforços. Face às suas atribuições, o CMCD é responsável pelo acompanhamento e monitorização do PDCCD 2019-2023, "assegurando a sua atualização nos próximos triénios" (MDN, 2020b, p.2). Entre outras atribuições, o CMCD deverá apresentar uma proposta de ENCD (em dois meses), um enquadramento jurídico-constitucional da atuação das FFAA (em três meses) e uma proposta de política de Recursos Humanos (RH) para a ciberdefesa (em três meses).

3.2. Enquadramento internacional

O número crescente de ciberataques, afetando vários Países, evidenciou a necessidade de desenvolver políticas cooperativas de combate a todas as formas de ataque cibernético, abordando de forma agregada as questões relacionadas com a cibersegurança e ciberdefesa.

A ciberdefesa surge pela primeira vez no conceito estratégico da NATO (2010), aprovado na cimeira de Lisboa. Em 2014, na cimeira de Gales, a Aliança reconheceu a aplicabilidade do direito internacional no ciberespaço (NATO, 2014a), identificando-o como área de confrontação estratégica. Na sequência desta decisão, face ao aumento das ameaças cibernéticas, a NATO (2014b) aprovou também a sua *enhanced policy on cyber defence*, prevendo a adoção de uma resposta conjunta, face a ataques puramente cibernéticos ou convencionais. Na sequência desta decisão, Portugal assinou em 2016 um memorando de entendimento na área da ciberdefesa que permitiu implementar mecanismos de cooperação e assistência ao nível da partilha de informação.

Na cimeira de Varsóvia, após o reconhecimento do ciberespaço como novo domínio das operações, Portugal ratificou também o *cyber defence pledge* (NATO, 2016a), assumindo o compromisso de reforçar a proteção das suas redes e infraestruturas, alocar recursos, robustecer as suas capacidades de ciberdefesa e a partilha de informação, promovendo a formação e o treino.

Na cimeira de Bruxelas (NATO, 2018a), no âmbito da revisão da sua estrutura de comando, a Aliança decidiu criar um *Cyberspace Operations Centre* (CyOC), diretamente dependente do *Allied Command Operations* (ACO), bem como a disponibilização voluntária de efeitos operacionais por parte de alguns Aliados, no quadro das missões e operações NATO.

Também neste domínio, a UE (2009) desenvolveu um conceito de ciberdefesa, ampliado e aprovado em 2012 (UE, 2012). De forma a reforçar a capacidade para fazer face a ciberataques, a UE divulgou um conjunto de medidas destinadas a incentivar os Estados-Membros a reforçar as suas capacidades de ciberdefesa, incluindo a possibilidade de estes submeterem projetos cooperativos no quadro da *PErmanent Structured Cooperation* (PESCO) e do Fundo Europeu de Defesa (FED). Envolvendo as universidades e os setores industriais e tecnológicos, salienta-se a participação nacional em projetos europeus no domínio da ciberdefesa, nomeadamente, liderando o Projeto *Cyber Academia and Innovation Hub* (CAIH).

Reconhecendo que 22 dos 30 países NATO fazem parte da UE, estas organizações decidiram também reforçar a sua parceria estratégica nesta área e assinaram na cimeira de Varsóvia uma declaração conjunta. A cibersegurança e a ciberdefesa foram assumidas como

áreas prioritárias de cooperação, sendo identificadas opções concretas, com efeito imediato: "de forma a fortalecer a cooperação na área do treino, a partir de 2017, a UE e a NATO vão harmonizar os requisitos de treino e abrir os respetivos cursos de formação à participação mútua do seu *staff* " (UE-NATO, 2016, p. A-6).

Para vencer este desafio, intimamente ligado à capacitação de quadros, importa referir que Portugal ocupa uma posição central numa rede de centros de excelência e polos de conhecimento nacionais e internacionais, decorrente da liderança do projeto NATO *Smart Defense Multinational Cyber Defence Education and Training* (MNCDE&T), da co-liderança da *Cyber Defence Discipline* da UE e da instalação da *NATO Communications and Information Academy* (NCI Academy) em Oeiras.

Alinhada com estes esforços, importa agora definir uma visão estratégico-militar para a ciberdefesa, orientadora da transformação organizacional, operacional e genética já em curso.

3.3. Definição da estratégia militar para o ciberespaço

O CEM e as LOENCD, refletindo a forma como o nível político-militar perspetiva a integração do ciberespaço na estratégia militar, constituem os fundamentos da visão estratégica que se pretende estruturar neste domínio.

As LOENCD definem como nível de ambição para a ciberdefesa, no período 2019-2023, que esta "assegura em permanência a proteção das infraestruturas da Defesa, a condução de OpCiber em apoio ao Sistema de Forças, incluindo as Forças e elementos Nacionais Destacados (FND), e contribui proactivamente para a segurança do ciberespaço de interesse nacional e a projeção internacional de Portugal" (MDN, 2019b, p.14-15). Estas, estabelecem também princípios, Linhas Orientadoras (LO) e Requisitos Estratégicos (RE), permitindo, a partir daí, deduzir os objetivos a atingir pela EMCIBER, conforme quadro em Apêndice E.

A informação recolhida a partir das entrevistas realizadas, cuja síntese se documenta no Apêndice D, permitiu percecionar tendências relativamente aos elementos (âmbito e finalidade) e componentes da EMCIBER (operacional, estrutural e genética).

Atendendo à sua natureza complementar e supletiva relativamente à ENCD, como uma das componentes da estratégia militar e a esta subordinada, a EMCIBER, pode ser definida como:

- A ciência e a arte de desenvolver e aplicar a coação militar no ciberespaço, com vista à consecução dos objetivos fixados pela Defesa Nacional (DN).

Na sua implementação, esta estratégia articula-se com as restantes estratégias militares particulares, respetivamente nos domínios naval, terrestre e aeroespacial.

3.4. Síntese conclusiva

Com base nas referências elencadas, elaborou-se uma síntese das características mais marcantes do quadro teórico enformador, tendo em vista a sua inclusão como contributos para a definição de uma EMCIBER.

Face à definição apresentada, conclui-se que a EMCIBER tem por âmbito: o emprego da coação militar no ciberespaço, tendo por fundamentos a defesa da soberania nacional e a salvaguarda dos interesses nacionais, conforme definido pelo poder político. Tendo por base o âmbito e as capacidades identificadas, considera-se que Portugal deve orientar a sua EMCIBER de forma a assegurar a garantia da informação, condição essencial para assegurar a resiliência e soberania nacional, estabelecendo como prioridade a defesa das redes militares e a condução de OpCiber, conforme prescrito pelas LOENCD.

Em resposta à QD1 (*Quais as componentes que, face ao impacto estratégico do ambiente da informação, deverão fazer parte da definição de uma EMCIBER*?), conclui-se que a definição da EMCIBER obriga à clarificação do seu âmbito de aplicação e da finalidade a atingir (nível de ambição), elementos que orientam e enquadram as suas componentes operacional, estrutural e genética. Resulta assim validada a H1 formulada.

4. Estratégia operacional para o ciberespaço

Combinando a existência de ameaças provenientes de atores Estado e não-Estado, o ciberespaço expõe vulnerabilidades civis e militares, requerendo respostas multidimensionais nos domínios civil-militar e nacional-internacional. Atendendo à utilização frequente do ciberespaço pelas ameaças híbridas e ao impacto crescente dos ciberataques, as FFAA necessitam de levantar uma capacidade credível para assegurar, de forma eficaz, a defesa do País neste domínio.

A proteção das redes da Defesa e a condução de OpCiber, constituem os "pilares" da componente operacional da EMCIBER. A compreensão da sinergia e interdependência existente entre estes elementos, permite deduzir um conceito de emprego operacional das FFAA e, a partir daí, alinhar a resposta estrutural (forças) e genética (meios) associada à sua ação.

Tendo a NATO assumido o ciberespaço como um novo domínio de operações em 2016, no âmbito da caracterização da EMCIBER, importa identificar qual o impacto desta decisão na condução das operações das FFAA, tanto sob o ponto de vista doutrinário como operacional. O objetivo a atingir é o de promover uma visão coerente, sinérgica e cooperativa da atuação das FFAA no ciberespaço, apoiando e integrando as atividades a desenvolver pelos diversos atores, nomeadamente, em situações de crise ou conflito.

4.1. Revolução tecnológica, ciberespaço e impacto militar

O paradigma social da era industrial, deu lugar a uma sociedade da informação, descentralizada e aberta, caracterizada pela incerteza. As estruturas em rede têm um forte efeito desagregador nas organizações hierarquizadas como as FFAA, originando a emergência de novos poderes. Estes, desafiam o poder do Estado tanto no plano interno como externo, provocando a sua "erosão", condicionando o exercício da cidadania, da governação e até da sua soberania.

Apesar de a ciberdefesa estar naturalmente ligada à segurança das redes e dos SIC, elemento estruturante e vital do C2 das operações militares, estes não constituem o único alvo dos ciberataques. A maior parte das capacidades militares e sistemas de armas depende, cada vez mais, do funcionamento em rede, constituindo também um alvo.

O nível de inovação e sofisticação, que caracteriza os novos vetores de ataque, com uma forte ligação aos "objetos da internet", à supercomputação (computação quântica) e à inteligência artificial, faz crescer exponencialmente a superfície de ataque e o nível da ameaça, introduzindo riscos difíceis de quantificar e avaliar em toda a sua extensão.

A agregação ao ciberespaço da robótica e das novas perspetivas e modelos de interação oferecidos pelas redes semânticas, terá também inevitáveis e fortes consequências no domínio

militar. Tal como já acontece no caso dos drones e das aeronaves não tripuladas, será expetável que, em breve, os combatentes venham progressivamente a ser substituídos por veículos e sistemas não tripulados. Nos conflitos do futuro, a intervenção do ser humano (o combatente) terá essencialmente lugar de forma remota, com uma limitada presença física no campo de batalha.

Impondo-se a utilização segura destas tecnologias emergentes, a proteção das redes amigas e a capacidade para assegurar a disrupção dos SIC do adversário, assume um papel crítico e central. O acompanhamento desta evolução será vital para o sucesso das FFAA nos futuros domínios de conflito, sejam estes de natureza física ou virtual.

4.2. Novo paradigma operacional: operações não-cinéticas e multi-domínio

Os conflitos entre Estados, de natureza simétrica, deram lugar a conflitos assimétricos, de curta duração, baixa intensidade e envolvendo múltiplos contendores. Caracterizados pelo uso limitado da força, estes assumem tendencialmente um carácter híbrido, explorando a produção simultânea de efeitos em vários domínios militares e não-militares, utilizando sobretudo meios não cinéticos que potenciam a utilização do ciberespaço.

Face ao atual quadro de empenhamento das FFAA e às características do ambiente operacional, existe um claro desajuste entre as capacidades e meios militares da era industrial, predominantemente cinéticos, e as requeridas pelos conflitos da era moderna. Estes, requerem, cada vez mais, a mobilização de capacidades de natureza não-cinética para a sua resolução, onde o desenvolvimento de OpCiber pode ser instrumental e decisivo, afetando outros domínios operacionais, muitas vezes sem a utilização de meios cinéticos.

Conforme refere a DMPDM, o "número crescente de atores com capacidade para intervir nos domínios terrestre, aéreo, marítimo, espacial e do ciberespaço (ambiente multi-domínio) representa um desafio adicional para a capacidade de resposta dos Estados e das organizações multilaterais de segurança" (MDN, 2020a). Esta nova visão doutrinária do ambiente de segurança, altera profundamente o conceito de operações conjuntas vigente, introduzindo a necessidade de cada componente perspetivar a sua ação não só no seu domínio, mas também nos restantes, obrigando a um planeamento de natureza transversal e interagência (Pires, 2018, p.16).

Sem prejuízo de atuar como componente combatente ou sinérgica, conforme ilustrado na Figura 5, o ciberespaço desempenha permanentemente o papel de força de proteção. Todas as atividades das FFAA, exigem assim uma aproximação multi-domínio, onde as restantes componentes, mesmo atuando de forma individualizada, devem incluir no seu planeamento a proteção no ciberespaço.

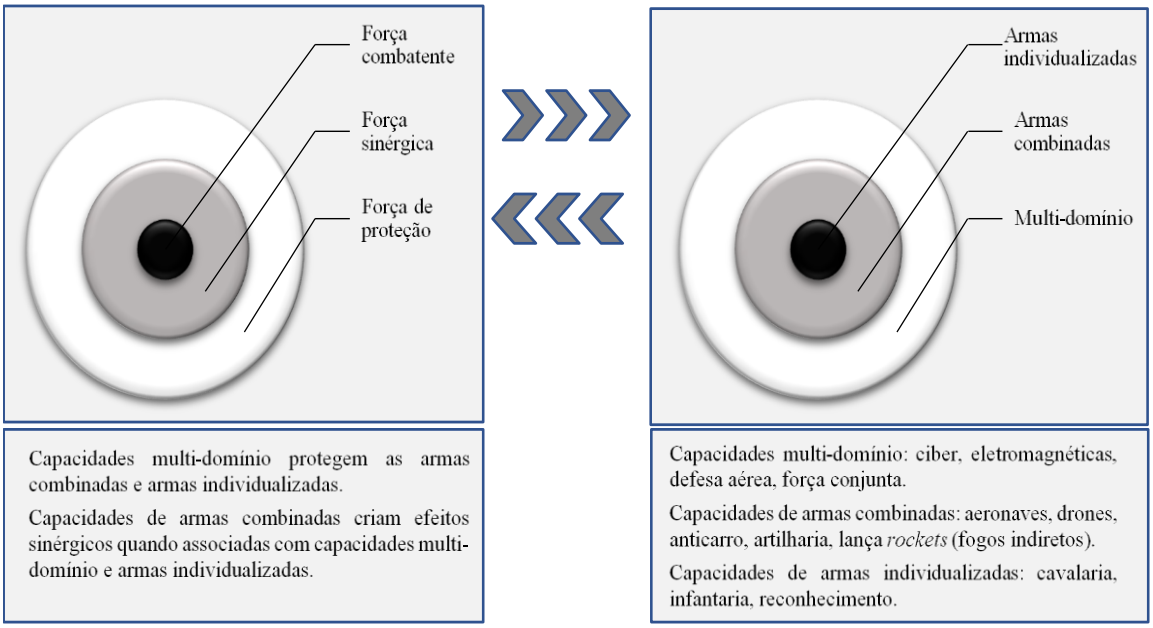


Figura 5 – Formações de combate multi-domínio

Fonte: Adaptado a partir de Fox (2017, p.34).

Transcendendo a sua componente infraestrutural (física), o ciberespaço estende também o seu impacto para o domínio virtual que, pela sua natureza, ultrapassa os limites geográficos do tradicional teatro de operações. A "área de interesse" no ciberespaço (Figura 6), revela-se muito mais extensa do que a área de operações conjunta, incluindo as redes das FFAA e da Defesa, redes nacionais e redes não-nacionais, onde também se encontram sistemas adversários e de não-aliados.

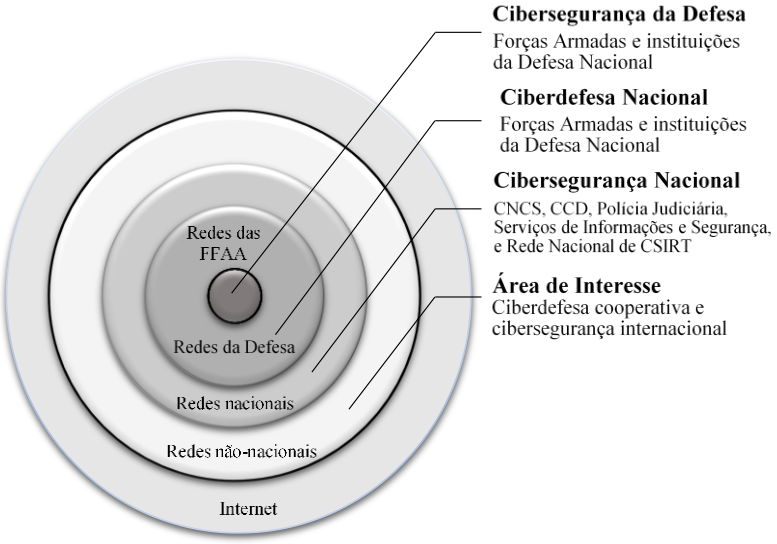


Figura 6 – Áreas de responsabilidade no ciberespaço

O reconhecimento do ciberespaço como novo domínio das operações consubstancia assim uma alteração do paradigma operacional, levando as FFAA a focar a sua atenção na

garantia do cumprimento da missão (*mission assurance*) em todos os domínios de atuação. Conforme a Figura 7, face ao impacto das OpCiber, uma postura essencialmente passiva e defensiva, orientada para a resiliência dos SIC e para a proteção do ciberespaço (resiliência Ciber), deve agora dar lugar a uma postura mais proativa (defensiva e ofensiva), assegurando a resiliência operacional das FFAA (garantia da missão).

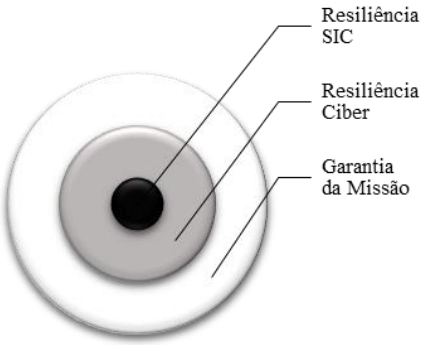


Figura 7 – Gestão da resiliência operacional no ciberespaço

Fonte: AJP-3.20 (2020, p.5).

Neste contexto, envolvendo redes e sistemas internos e externos às FFAA, as OpCiber envolvem medidas passivas e ativas (Figura 8), cobrindo diversas áreas, de âmbito e natureza diferenciada, de caráter defensivo e/ou ofensivo, exclusivo e específico das FFAA.

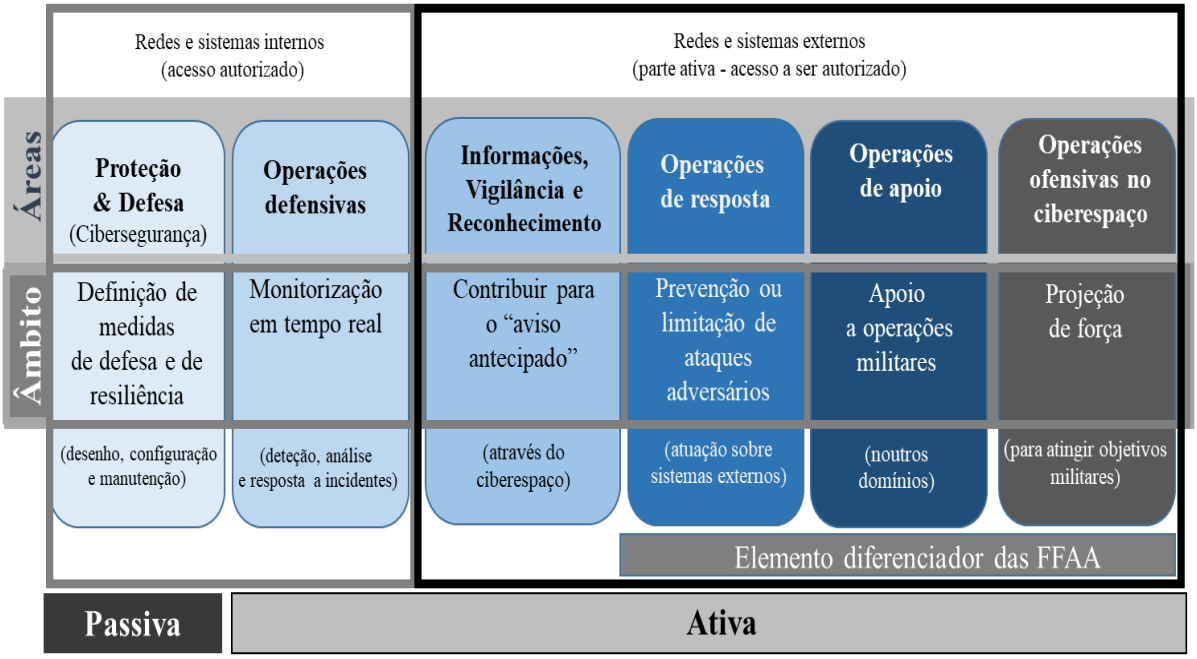


Figura 8 – Enquadramento e contexto das operações no ciberespaço

Fonte: Adaptado a partir de EMGFA (2019b) e NLD-MOD (2018).

De espectro alargado, estas medidas oferecem aos comandantes militares mais meios/ferramentas operacionais, maior flexibilidade/proporcionalidade na resposta e uma maior liberdade de ação.

Relativamente à maturidade doutrinária, demonstrada para apoiar este conceito de emprego de forças, a perceção dos entrevistados é a de que a situação atual ainda revela uma visão tática/técnica, de natureza puramente defensiva, focalizada essencialmente na resiliência dos SIC. Relativamente à situação desejável, a atingir futuramente, a tendência recolhida foi a de que deveria ser adotada uma visão doutrinária de nível estratégico-militar (resiliência operacional das FFAA) ou de nível político-estratégico (resiliência nacional). O facto de existir uma diferença assinalável entre a perceção da situação atual e futura, demonstra a urgência de uma alteração substantiva dos fundamentos doutrinários vigentes.

4.3. Planeamento operacional

O ciberespaço é, pela sua construção antrópica, um domínio de operações diferente dos restantes domínios naturais (terra, mar, ar e espaço). As OpCiber conferem vantagens significativas, nomeadamente, porque conseguem produzir efeitos imediatos, capazes de atingir, simultaneamente e à escala global, todos os domínios e níveis operacionais. Essencialmente por esta razão, as OpCiber são hoje perspetivadas como um multiplicador de forças.

No contexto do planeamento conjunto, o ciberespaço oferece assim novas possibilidades operacionais, produzindo efeitos de natureza dual física/virtual. Conforme ilustrado na Figura 1, enquanto algumas OpCiber suportam a condução de operações de informação, outras apoiam ações cinéticas, atingindo objetivos específicos nos domínios físicos.

Na utilização de OpCiber, caracterizadas pelas suas três dimensões (física, lógica e cognitiva) deve evitar-se o impulso de simplificar e limitar o seu planeamento e execução à dimensão física. Ao não considerar a sua componente lógica e cognitiva, reduzir-se-á drasticamente a probabilidade de sucesso e a capacidade de sobrevivência das FFAA num campo de batalha iminentemente digital.

O planeamento de OpCiber segue os mesmos princípios do processo de planeamento operacional NATO (AJP-5.0, 2019).

4.3.1. Processo de planeamento operacional

Com a inclusão do ciberespaço na estratégia militar, a articulação operacional das FFAA, nos vários domínios e áreas de responsabilidade, deverá ser reequacionada. Devido à sua natureza transversal/multidimensional e aos riscos de "fratricídio" no ambiente da informação, o ciberespaço impõe a necessidade de garantir, permanentemente, a coordenação estratégica e operacional de todas as ações nele produzidas. Daqui decorre que os "efeitos no ciberespaço são melhor planeados e executados ao nível estratégico e operacional, através de um C2 centralizado" (NATO, 2019d, A-4).

O processo de planeamento de OpCiber dá resposta à necessidade de integrar capacidades e efeitos neste domínio, contrariando a sua livre utilização por adversários, defendendo redes críticas e atingindo objetivos essenciais para o cumprimento da missão das FFAA. Pretende também assegurar a "operação num ambiente degradado, a utilização de recursos limitados e consolidar os requisitos operacionais para a utilização de efeitos no ciberespaço" (AJP-3.20, 2020, p.23).

Apesar dos seus aspetos específicos, o planeamento de OpCiber não difere muito do de outras operações, seguindo, na sua articulação, a *Comprehensive Operations Planning Directive* (COPD) NATO (2013). Os seus princípios orientadores podem ser aplicados a todos os níveis de planeamento (estratégico, operacional e tático), em todas as fases da COPD e a todos os tipos de OpCiber (defensivas e ofensivas).

O planeamento operacional segue o planeamento do nível estratégico-militar e é conduzido essencialmente ao nível do Comando Conjunto e dos Comandos de Componente que o apoiam ou que a este se encontram subordinados. Este processo compreende seis fases, conforme se apresenta na Figura 9.

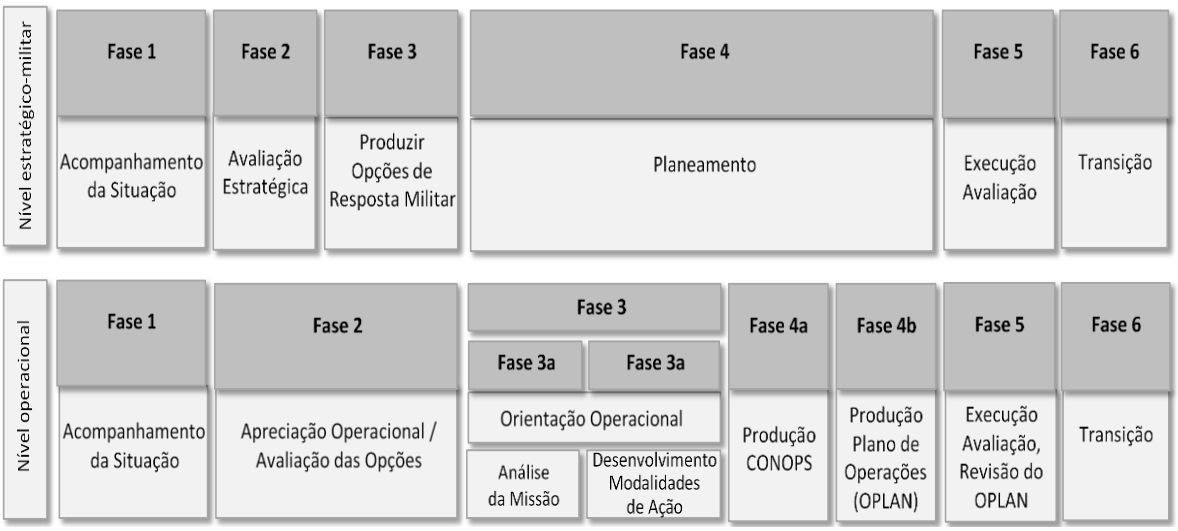


Figura 9 – Fases do planeamento operacional

Fonte: NATO (2013).

Articuladas sequencialmente, estas fases garantem a estreita colaboração entre todos os níveis de comando, durante as diferentes etapas de gestão de uma crise. O alinhamento deste processo assegura também que a orientação estratégica é estabelecida de forma a assegurar o sucesso operacional.

A dimensão cibernética dos "conflitos híbridos", cujos atores envolvidos e vetores de ataque são pouco visíveis, vem reforçar a necessidade de adoção de uma aproximação interagência, assegurando a cooperação civil-militar aos vários patamares de decisão, nomeadamente, para enfrentar o novo espectro da ameaça.

4.3.2. Conceito de emprego e C2 das operações no ciberespaço

O reconhecimento do ciberespaço como novo domínio das operações pelas FFAA, traduz-se no desenvolvimento da sua capacidade militar para assegurar a Defesa do País neste domínio de uma forma tão eficaz como o fazem no mar, terra ou ar, mantendo permanentemente a sua capacidade de C2 e a liberdade de ação, assegurando assim a condução de operações militares em todos os domínios e circunstâncias.

Decorrendo da sua visão operacional para o ciberespaço (NATO, 2017), a Aliança desenvolveu um Conceito de Operações (CONOPS), definindo um conjunto de princípios orientadores para o exercício do C2 (NATO, 2019c). Em linha com este documento, define-se no Apêndice F um conceito de emprego das FFAA no ciberespaço. Este conceito, genericamente detalhado, caracteriza a articulação das FFAA na condução de OpCiber e as relações de C2 entre todos os níveis de comando, facilitando assim a elaboração de um CONOPS específico para cada missão, tarefa ou operação.

Uma vez que as OpCiber transcendem os limites físicos do território nacional e envolvem áreas fora do controlo das FFAA, a implementação do conceito de emprego e das relações de C2 formuladas, requer uma estreita coordenação com os outros instrumentos do poder nacional e domínios de operações das FFAA. O conjunto de respostas a adotar pode também ultrapassar a esfera militar tendo, neste caso, que respeitar a soberania de outros Estados e o direito internacional.

4.3.3. Regras de empenhamento

Na condução de OpCiber, o comandante operacional terá que considerar todas as limitações e/ou constrangimentos existentes, nomeadamente, os de natureza política ou legal. Neste contexto, deverá existir um claro entendimento da legislação internacional e nacional aplicável e das regras de empenhamento associadas à utilização de efeitos no ciberespaço.

No âmbito NATO, o quadro legal aplicável e a autoridade para conduzir OpCiber depende da natureza e contexto das ações a desenvolver (AJP-3.20, 2020, p.19), incluindo:

- um plano de operações aprovado pelo *NATO Allied Council* (NAC), que inclui regras de empenhamento para as OpCiber, conforme aplicáveis;
- a autoridade conferida ou política existente;
- os efeitos esperados com a condução das OpCiber;
- a indicação do seu enquadramento, referindo se estas operações são conduzidas durante um conflito armado, num contexto de legítima defesa, ou no âmbito de outras operações ou missões que se situem abaixo do limiar de um conflito armado; e
- identificação do tipo de operações, especificando se estas são defensivas ou ofensivas.

Face ao enquadramento apresentado, um ataque militar só será legítimo e legal se for dirigido a objetivos militares. A condução de OpCiber deve assim ter em conta que alguns SIC são de uso duplo (militar e civil), tornando difícil identificar a sua elegibilidade como alvos militares. Entre outros aspetos, uma prévia estimativa dos danos colaterais, a aplicação dos princípios da neutralidade e da distinção/descriminação dos alvos, será determinante para assegurar a legitimidade destas operações.

A atribuição da responsabilidade legal pela condução de ciberataques revela-se também especialmente difícil, nomeadamente, devido à elevada probabilidade de serem utilizados métodos dissimulados, explorando técnicas de deceção que apontam para entidades terceiras. Os desafios associados à atribuição apresentam importantes implicações legais, influenciando decisivamente a formulação de uma resposta militar.

Respeitando as responsabilidades e competências legais atribuídas às várias entidades envolvidas na cibersegurança e ciberdefesa nacional, sempre que necessário, deverá ser realizada uma avaliação conjunta da sua atuação no contexto de uma operação militar no ciberespaço. Se aplicável, no quadro da defesa coletiva e de uma atuação cooperativa no contexto das organizações internacionais de que Portugal faz parte, deverá também ser tido em consideração o possível envolvimento de outras nações aliadas.

Pela sua importância para a atuação das FFAA, aprofunda-se no Apêndice G o enquadramento legal do uso da força no ciberespaço e o seu enquadramento jurídico nacional.

4.4. Síntese conclusiva

Confirmando a natureza das implicações operacionais do reconhecimento do ciberespaço como novo domínio das operações para as FFAA, foi possível constatar que para a generalidade dos responsáveis pela ciberdefesa nacional (ver Apêndice D), situados aos diversos níveis de planeamento, o ciberespaço é fundamental para a realização de qualquer tipo de operação militar, independentemente da conjuntura e/ou situação. Neste contexto, as OpCiber devem ser planeadas ao nível estratégico-operacional e executadas ao nível operacional e tático, envolvendo a condução de operações defensivas e ofensivas.

Em resposta à QD2 (*Qual é, ao nível da estratégia operacional, o impacto do reconhecimento nacional do ciberespaço como quarto domínio das operações?*), conclui-se que o reconhecimento e formalização da componente operacional da EMCIBER requer a definição de um quadro doutrinário orientador e de um conceito de emprego operacional de forças e meios no ciberespaço (CONOPS). Desta conclusão decorre a validação da H2.

5. Estrutura nacional de ciberdefesa

Assim como existe uma estreita ligação entre a Segurança e a DN, também a cibersegurança se revela indissociável da ciberdefesa do Estado, exigindo não só o desenvolvimento de estruturas especificas, mas também uma visão integrada e sinérgica. Como elemento estruturante da implementação da EMCIBER, indissociável deste processo, encontra-se a definição das relações de C2 a estabelecer (Apêndice F) e a revisão orgânica, já em curso no EMGFA (2018b).

Procurando garantir o alinhamento entre a componente estrutural e operacional da EMCIBER, caracterizam-se as estruturas orgânicas existentes e o nível em que decorre a integração de capacidades operacionais. Com base na perceção recolhida a partir das entrevistas realizadas e do tratamento qualitativo e quantitativo dos dados obtidos, definem-se tendências e formulam-se propostas.

5.1. Estruturas e modelos de referência internacionais

A cena internacional no domínio da ciberdefesa é dominada por um conjunto de atores particularmente poderosos, onde se distinguem os países anglo-saxónicos (Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia), a Rússia, China, Israel, Alemanha e a França. A maioria destes países iniciou, essencialmente a partir de 2000, uma reflexão estratégica estruturante que gerou, à escala mundial, uma dinâmica de desenvolvimento de capacidades neste domínio. No ciberespaço, as potências são assim pouco numerosas, mas facilmente identificáveis.

Na cimeira de Bruxelas, a NATO (2018a) reconheceu a necessidade de estabelecer uma estrutura de comando ajustada ao atual ambiente de segurança, incluindo a criação do CyOC, no ACO. Decorrendo dos compromissos internacionais assumidos, Portugal enfrenta também o desafio de edificar as suas capacidades e estruturas nacionais, reforçando não só a resiliência nacional, mas também a cibersegurança e ciberdefesa cooperativa.

De forma a melhor enquadrar a visão estrutural a adotar na implementação da EMCIBER, optou-se por analisar a aproximação seguida por um conjunto de países que, pela sua dimensão e afinidade com a situação nacional, permitissem recolher referências úteis para este estudo. Nos aspetos relacionados com a transformação orgânica operada no contexto NATO (2018a; 2019a) e noutras nações aliadas, foi analisado o caso dos Estados Unidos da América (EUA) (Pernik & Verschoor-Kirss, 2016), Alemanha (Hoffmann, 2019), Reino Unido (Osula, 2015), França (Brangetto, 2015), Itália (ITA-CS, 2017), Espanha (Cendoya, 2016) e Holanda (Wieriks, 2018).

Como denominador comum a todos os países, constatou-se que foram criados Comandos para as OpCiber, diretamente dependentes do comandante das FFAA (nível

CEMGFA). Com autonomia para realizar OpCiber e produzir efeitos estratégicos e operacionais, estas estruturas assumem-se como Comando de Componente (apoiante ou apoiado) num contexto operacional conjunto.

Relativamente à estrutura orgânica, é adotada uma lógica semelhante ao nível das áreas de estado-maior e operações, alinhada com as melhores práticas NATO. À exceção do caso dos EUA[2] e da Alemanha[3], os restantes países apresentam uma organização muito idêntica (EMGFA, 2019b), contemplando a existência de:

- um centro de operações: assegura a defesa dos SIC e do C2 das FFAA e da DN, funcionando em permanência segundo uma lógica de *Computer Emergency Response Team* da Defesa (CERT.DEF);
- um estado-maior: garante a gestão/coordenação das atividades de planeamento e execução, incluindo o desenvolvimento de capacidades e a sua articulação operacional tanto ao nível nacional como internacional, no quadro da ciberdefesa cooperativa;
- uma estrutura técnica: coordena a análise de incidentes e o exercício da autoridade técnica no âmbito da ciberdefesa nacional e da cibersegurança na área da Defesa;
- uma componente operacional: com capacidade ofensiva e dotada de equipas permanentes, orientadas para: a execução de CNO (nas suas várias vertentes), complementando as capacidades do CERT.DEF; ligação aos restantes Comandos de Componente e ao Comando Conjunto das operações militares.

Esta análise, permitiu identificar o enquadramento institucional, a articulação operacional e as áreas funcionais estruturantes que, concorrendo para um novo modelo organizacional, constituem elementos de referência a ter em conta na adaptação/transformação das estruturas nacionais existentes.

5.2. Situação nacional

Na sequência da aprovação da reforma "Defesa 2020", na estrutura orgânica do EMGFA, foi criado, em 2015, o CCD das FFAA. Dependente da Direção de Comunicações e Sistemas de Informação (DIRCSI), o CCD constitui o ponto focal da CCDFFAA e da estrutura nacional de ciberdefesa.

Através das entrevistas realizadas e da informação recolhida, constatou-se que este posicionamento institucional, refletindo uma visão essencialmente técnica, não favorece a

[2] O *US Cyber Command* constitui um comando combatente desde 2010, cujo comandante é também o Diretor da *National Security Agency*.
[3] Criou em 2016 um novo Ramo das FFAA designado por *Cyber and Information Domain Service*.

integração da área da ciberdefesa no planeamento conjunto. Apesar da responsabilidade pela integração de capacidades operacionais estar atualmente centralizada no CCD, a sua coordenação é realizada de forma distribuída através dos Ramos, sem permitir a necessária unidade de comando e esforço.

As estruturas existentes nos Ramos, afetas às áreas da cibersegurança e da ciberdefesa, apresentam também estruturas e enquadramento funcional diferente, não permitindo assegurar uma operação continua (24 horas/sete dias). Este facto, associado à não existência de doutrina e procedimentos técnicos consolidados, dificulta a integração e articulação operacional das capacidades existentes. A condução eficiente e eficaz de todo o espetro das CNO (defensivas, exploração e ofensivas), é considerada um pré-requisito para o desenvolvimento de OpCiber, requerendo um alinhando da resposta genética e operacional da ciberdefesa.

Tanto ao nível do CCD como das estruturas *Computer Incident Response Capability* (CIRC) dos Ramos, assinala-se a existência de um número reduzido de RH qualificados, registando-se também dificuldades de recrutamento e retenção de quadros, essencialmente devido a constrangimentos na gestão de carreiras e na progressão horizontal. Estas limitações/lacunas são comuns tanto às estruturas nacionais de cibersegurança como de ciberdefesa.

Face aos novos desafios operacionais e às implicações doutrinárias daí decorrentes (nacionais, NATO e UE), torna-se necessário, com a maior brevidade possível, ajustar as estruturas orgânicas existentes, promovendo um incremento quantitativo e qualitativo de pessoal de forma a reforçar as capacidades CNO das FFAA. O PDCCD (EMGFA, 2019b), recentemente aprovado, perspetiva esta evolução, tendo o CCD adotado uma estrutura transitória até 2020-2021.

5.3. Alinhamento da resposta estrutural

Complementando a análise da situação atual, importa agora perceber como promover a adaptação da estrutura nacional de ciberdefesa aos requisitos operacionais existentes. Neste âmbito, através das perceções recolhidas (Apêndice D), foi possível identificar tendências, refletindo a necessidade de garantir o alinhamento da estrutura orgânica com o nível em que se materializa doutrinariamente a integração das capacidades operacionais de ciberdefesa.

No contexto das FFAA, conforme reconhecido pelos entrevistados, a dependência de uma entidade técnica (DIRCSI) limita o âmbito de atuação e a condução de OpCiber. A resposta estrutural da EMCIBER deve, por esta razão, ser conjunta, autónoma e situar-se na dependência direta do CEMGFA, assumindo a forma de um Comando de Operações no Ciberespaço (COCIBER), incluindo militares e civis.

Ainda segundo os entrevistados, o objetivo da edificação da CCDFFAA não será atingido sem pessoal qualificado, capaz de assegurar a condução de todo o espetro de CNO, comprometendo esta situação a capacidade de as FFAA conduzirem OpCiber. É, por esta razão, proposta a criação de um quadro especial de pessoal para a ciberdefesa, acautelando a progressão de carreiras, o recrutamento e a retenção de quadros, assegurando a formação e qualificação dos RH. Em linha com a ENSC, a atuação das FFAA deve ser também articulada de forma colaborativa com as restantes entidades com responsabilidades na segurança do ciberespaço.

A Figura 10 ilustra a correlação existente entre a média das respostas obtidas do questionário aplicado ao 3.º CPOCIBER e à Q3 (maturidade doutrinária) e Q5 (integração de capacidades operacionais) da entrevista, refletindo a perceção recolhida dos diferentes grupos ao nível: tático/técnico; operacional; estratégico-militar e estratégico nacional.

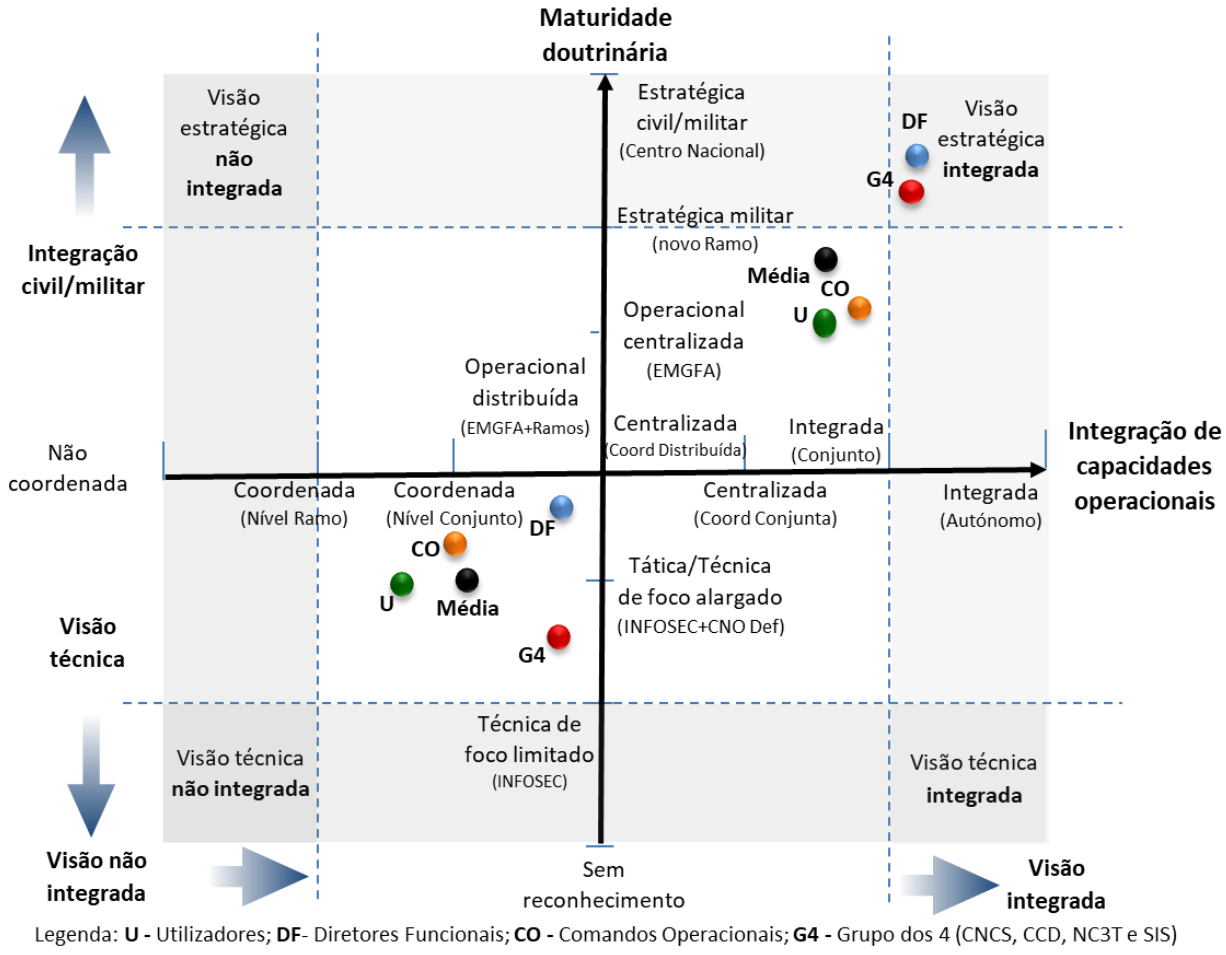


Figura 10 – "Maturidade doutrinária" *vs.* "integração de capacidades operacionais"

Relativamente à convergência dentro de cada grupo e intergrupal (Apêndice C), importa salientar que, apesar das divergências respeitantes à situação atual, existiu uma assinalável convergência relativamente à situação futura que se pretende promover.

Confirmando o enquadramento orgânico apresentado, em linha com a visão doutrinária proposta, os decisores situados aos níveis mais elevados, consideram que a integração de capacidades operacionais, atualmente centralizada no EMGFA, mas coordenada através dos Ramos, deverá evoluir para um modelo integrado, ao nível conjunto (Comando de Componente) ou até de forma autónoma (novo Ramo).

Neste quadrante (ver Figura 10), é percetível uma tendência doutrinária de futura aproximação civil-militar, de onde poderá vir a surgir a opção de co-localizar o centro de operações do COCIBER com o CNCS.

5.4. Estrutura nacional de ciberdefesa - visão futura

Tendo por base a visão expressa nas LOENCD (2019) e na DEEMGFA (2018), será de esperar que, no curto prazo, a atual estrutura do CCD (transitória) evolua para um COCIBER. Neste contexto, o modelo orgânico, conforme proposto e em aprovação pelo CEMGFA (Figura 11), reflete um nível de ambição ajustado à realidade nacional e encontra-se alinhado com as melhores práticas implementadas por outros Países Aliados.

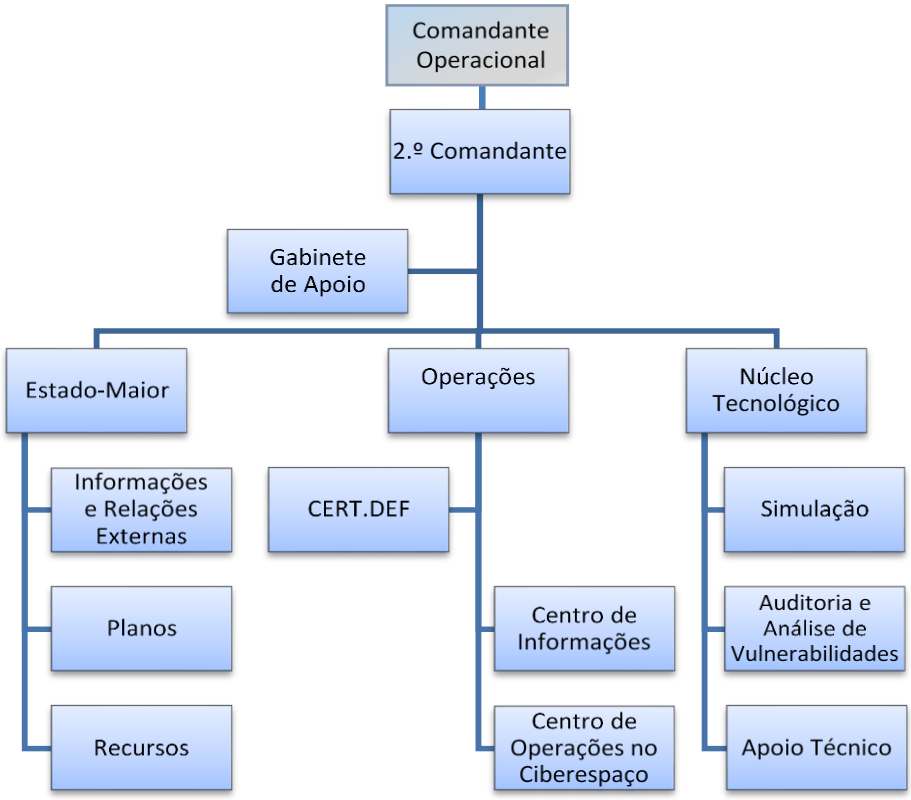


Figura 11 – Organização proposta para o COCIBER

Fonte: Adaptado de EMGFA (2019b).

De forma a garantir os RH adequados às necessidades estruturais da capacidade de ciberdefesa e a ultrapassar os constrangimentos identificados (EMGFA, 2019b), tanto ao nível do EMGFA como dos Ramos, propõe-se:

- a criação de um quadro especial para pessoal que integre a ciberdefesa, de forma a garantir a capacidade CNO e acautelar a progressão vertical (satisfação das condições especiais de promoção) e horizontal na carreira;
- o reforço do recrutamento de pessoal, explorando diferentes formas de prestação de serviço, incluindo a possibilidade de contratação de civis;
- a retenção de pessoal, alargando o período de inamovibilidade (até cinco anos), definindo um plano de incentivos e assegurando a formação e qualificação dos quadros;
- a definição de programas de formação e qualificação orientados para o desempenho de funções técnicas e para a condução de CNO, explorando a celebração de protocolos com instituições de Investigação, Desenvolvimento e Inovação (ID&I), instituições académicas e com a indústria;
- a constituição de uma reserva nacional para a ciberdefesa, integrando voluntários, militares e civis, tecnicamente qualificados.

Requerendo mecanismos de governação transversais, capazes de garantir a necessária articulação entre a cibersegurança e a ciberdefesa nacional, a atuação eficaz das FFAA no ciberespaço só será possível através da criação de uma cooperação alargada, ao nível público-privado, civil-militar e nacional-internacional. Conforme se apresenta na Figura 12, importa perspetivar as estruturas existentes segundo um modelo agregado, capaz de explorar sinergias nacionais e a cooperação internacional (NATO e UE).

A partir da observação deste modelo, em que o COCIBER assume um papel central na ciberdefesa nacional, as FFAA relacionam-se com várias entidades externas, criando aos vários níveis e patamares de decisão (estratégico, operacional e tático) comunidades de interesse horizontais.

Para assegurar o sucesso na condução de OpCiber, deve existir ao nível operacional uma ligação permanente do COCIBER (CERT.DEF) ao NATO CIRC (domínio da ciberdefesa) e do CNCS (CERT.PT) ao CERT.EU (domínio da cibersegurança). Ao nível tático/técnico, o CERT.DEF e o CERT.PT, integrando ambos a Rede Nacional de CSIRT, atuam de forma sinérgica tanto no âmbito da cibersegurança como da ciberdefesa.

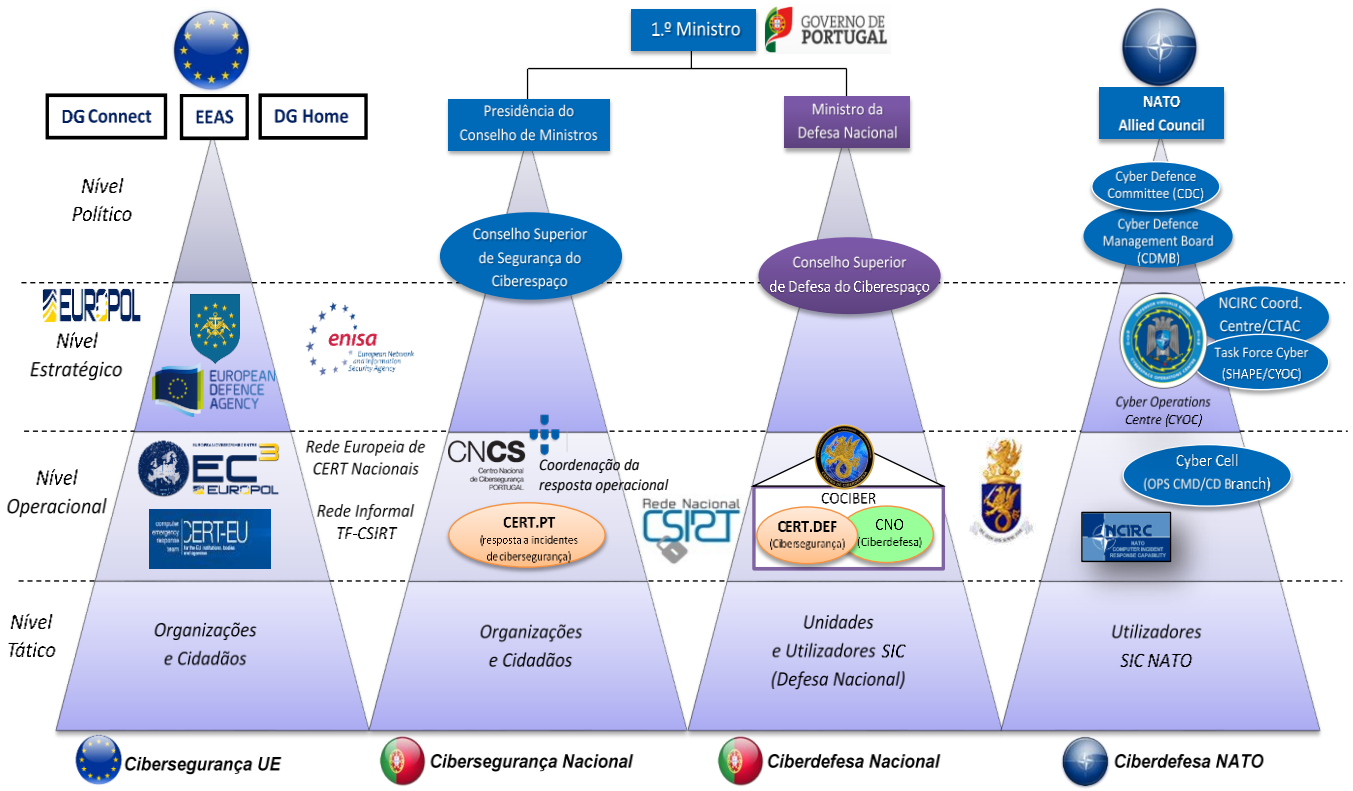


Figura 12 – Estrutura nacional de ciberdefesa e sua articulação internacional

Fonte: Adaptado a partir de Nunes (2018, p.72).

Analisadas as várias estruturas existentes ao nível político-estratégico, tanto no âmbito nacional como internacional (NATO e UE), identificam-se aproximações diferentes. No contexto NATO, a relação entre as várias entidades e estruturas orgânicas é definida com maior clareza tanto ao nível estratégico (CyOC, *NCIRC Coordination Center e Task Force Cyber*) como político (*Cyber Defence Committee* e *Cyber Defence Management Board*). No contexto nacional, esta ligação é assegurada pelo CSSC, conforme artigos 5.º e 6.º da Lei n.º 46/2018, de 13 de agosto.

Com base neste enquadramento orgânico, a estrutura de ciberdefesa das FFAA deve ser capaz de assegurar a transição de uma situação de normalidade para uma situação de crise ou conflito/guerra de forma flexível, com um tempo de alerta e transição reduzidos. As relações de C2, devem por isso ser ajustadas a cada situação, variando de acordo com as responsabilidades e autoridade atribuídas a cada entidade/organização do Estado.

Essencialmente por esta razão, como ponto central de coordenação político-estratégica da ciberdefesa nacional, conforme ilustrado na Figura 12, deverá ser criado um Conselho Superior de Defesa do Ciberespaço (CSDC). Em coordenação permanente com o CSSC, ao CSDC competirá promover a necessária articulação de esforços ao nível político-estratégico, acompanhar a implementação da ENCD, monitorizar o PDCC e facilitar a cooperação internacional na área da ciberdefesa, tanto no âmbito NATO como da UE.

A título de referência adicional, importa salientar que a estrutura agora proposta foi adotada no contexto do exercício "Ciber Perseu" (EME, 2015; 2018), tendo a mesma sido aplicada com sucesso no contexto da resposta nacional a uma situação de crise no ciberespaço[4].

5.5. Síntese conclusiva

A resposta estrutural apresentada, assegurando a necessária unidade de comando e esforço, dá resposta aos requisitos levantados pela componente operacional da EMCIBER. A nova ambição, partilhada por esta investigação, passa pela melhoria da eficiência dos processos associados à proteção dos SIC e à garantia da resiliência operacional das FFAA, reforçando substantivamente a sua eficácia operacional em prol da ciberdefesa nacional.

Em resposta à QD3 (*De que forma se pode, atendendo aos constrangimentos dos RH das FFAA e aos diferentes modelos orgânicos existentes, promover o levantamento da estrutura nacional de ciberdefesa?*), conclui-se que, em linha com os modelos orgânicos de referência e a transformação organizacional já em curso nas FFAA, será necessário estabelecer uma nova organização conjunta, autónoma, na dependência direta do CEMGFA, capaz de assegurar as funções de comando de componente/domínio operacional. A estrutura a adotar deverá incluir militares e civis. Para ultrapassar os constrangimentos de RH existentes nas FFAA e as dificuldades que estes colocam ao pleno desenvolvimento das capacidades CNO, propõe-se: a criação de um quadro especial para a ciberdefesa, de forma a acautelar a progressão de carreiras; o reforço do recrutamento e da retenção de talentos, assegurando a formação e qualificação do pessoal afeto a esta área. Adicionalmente, deverá ser pensada a constituição de uma reserva nacional para a ciberdefesa, integrando voluntários, militares e civis tecnicamente qualificados.

Ao nível da coordenação político-estratégica da ciberdefesa nacional, considera-se relevante a criação de um CSDC. Através das alterações estruturais propostas, a implementar no curto-prazo, será possível obter benefícios operacionais e genéticos concretos na condução de OpCiber, explorando para esse efeito sinergias e a cooperação com entidades externas às FFAA, tanto no plano nacional como internacional.

Confirma-se assim a H3 levantada.

[4] Ciberataque de larga escala lançado por um Estado sobre as infraestruturas críticas nacionais.

6. Geração de capacidades: a edificação da capacidade de ciberdefesa nacional

6.1. Enquadramento

A Diretiva Ministerial de Orientação Política para o Investimento na Defesa (MDN, 2018) definiu, como linha orientadora, o "investimento decisivo nos RH e materiais, para dotar as FFAA de uma capacidade nacional de ciberdefesa de excelência, como dimensão operacional prioritária e fundamental das FFAA". Incorporando esta orientação, a DEEMGFA 2018-2021 estabeleceu como objetivo estratégico o reforço e dinamização desta capacidade.

No quadro do esforço nacional de modernização das FFAA, a revisão da LPM (2019) priorizou também o investimento na edificação da CCDN. Como princípios orientadores, foram identificados a interoperabilidade, a flexibilidade, a adaptabilidade e o duplo-uso. A necessidade de reforçar as sinergias nacionais e a competitividade da indústria nacional, foi também salientada como requisito fundamental.

A edificação da CCDN, decorrendo da implementação da EMCIBER, deverá estar alinhada com as suas componentes genética, operacional e estrutural. Tendo por base este princípio enquadrador, o modelo proposto (ver Figura 2) analisa os vários vetores de desenvolvimento da capacidade segundo estas três perspetivas.

6.2. Processo de desenvolvimento da capacidade

O Processo de Desenvolvimento de Capacidades (PDC) NATO (*NATO Defense Planning Process,* 2020) e da UE (*Capability Development Plan* [CDP], 2018), é idêntico e encontra-se alinhado. Assegurando a convergência e potenciando os esforços a desenvolver por Portugal no quadro destas organizações, a DMPDM (2019-2022) assume que "o Ciclo de Planeamento de Defesa Militar (CPDM), orientado para o desenvolvimento de capacidades militares, deverá ser sincronizado e articulado com o ciclo de planeamento NATO e com o PDC da UE" (MDN, 2020a).

Atendendo ao nível de ambição estratégica definido e às diretivas/orientações existentes, o ciclo de desenvolvimento da CCDN é genericamente caracterizado na Figura 13.

Num esforço para assegurar a relevância e eficácia operacional no ciberespaço, as FFAA são continuamente confrontadas com a necessidade de melhorar as suas capacidades e preencher as lacunas existentes, reduzindo assim o risco operacional a que estão sujeitas. Atendendo às vulnerabilidades existentes, será necessário definir um PDC.

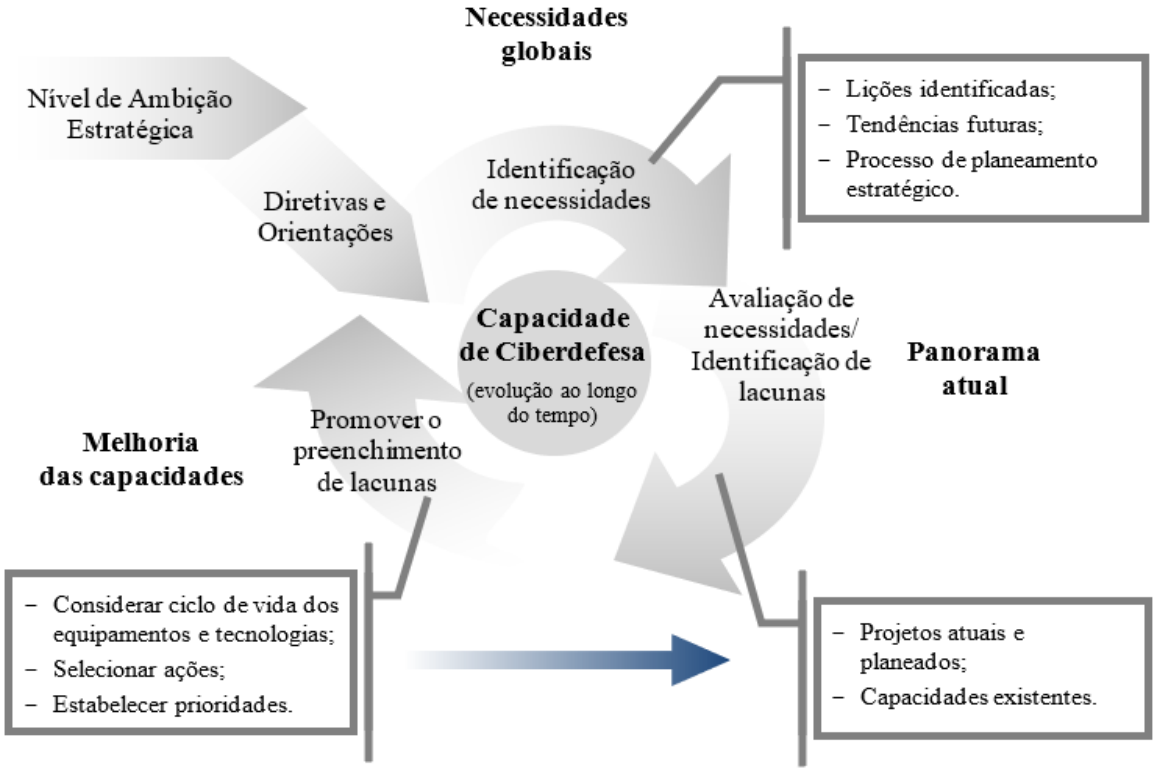


Figura 13 – Ciclo de desenvolvimento da CCDN

Fonte: Adaptado a partir de CDM (2003).

Tendo por fundamento os princípios formulados (*Capability Development Mechanism* [CDM], 2003; CDP, 2018), o desenvolvimento da CCDN pode ser articulado ao longo de quatro Linhas Estruturantes (LE):

- Identificação de lacunas e análise do seu risco operacional (LE A);
- Visão estratégica e tendências futuras (LE B);
- Planos e projetos de desenvolvimento de capacidades (LE C);
- Lições identificadas/aprendidas (LE D).

Apesar das LE identificadas se desenvolverem em paralelo, estas não podem ser equacionadas de forma isolada e desenquadrada. Em conjunto, constituem os blocos estruturantes do processo de desenvolvimento da CCDN. Conforme refletido no exemplo da Figura 14, a execução de uma determinada tarefa operacional pode ser influenciada pelas lições identificadas/aprendidas (LE D) e condicionada, ao longo do tempo, pelas restantes LE. Interagindo de forma integrada, as LE estabelecem a ponte entre o planeamento e a realidade, ao mesmo tempo que se conciliam os objetivos de curto com os de longo prazo.

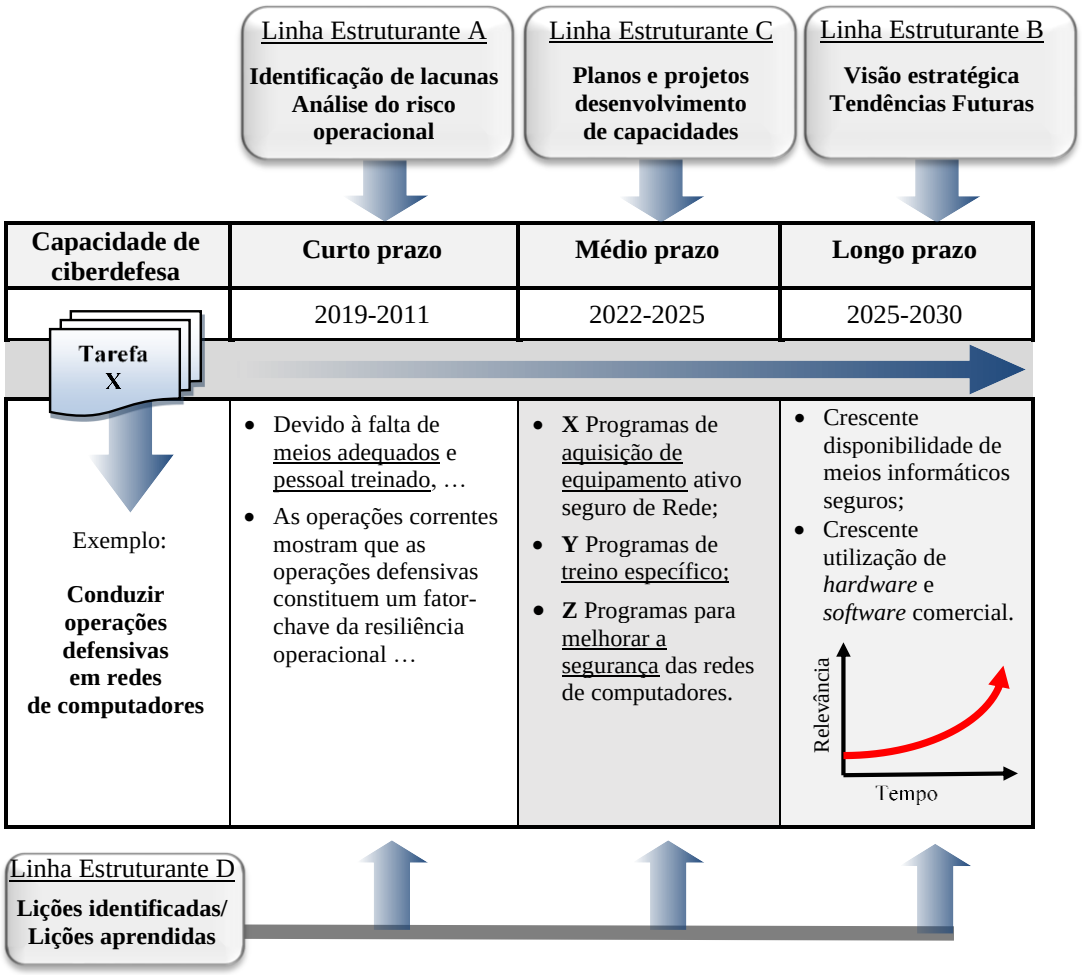


Figura 14 – Linhas de ação estruturantes do desenvolvimento da capacidade

Fonte: Adaptado a partir de CDP (2018) e Nunes (2015,-p.243).

Este "mecanismo", materializando um conjunto de passos sequenciais, permitirá atingir o nível de ambição estratégico definido, com os requisitos da capacidade preenchidos, reduzindo o risco operacional associado às lacunas existentes. Tendo como referência o que se pretende atingir e os recursos disponíveis, considera-se que este processo permitirá identificar, priorizar e gerir os desafios associados ao desenvolvimento da CCDN.

6.3. Plano de implementação da capacidade de ciberdefesa

É hoje consensualmente assumido que uma capacidade militar resulta da combinação de diversos elementos materiais e não-materiais, tradicionalmente designados como vetores de capacidade: Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLPII). Facilitando a implementação do processo de gestão de lacunas, este modelo permite equacionar diferentes possibilidades para o seu preenchimento.

Este processo holístico (Figura 15), identifica de forma mais clara e realista os elementos/áreas que estão na génese das lacunas existentes, assim como as suas dependências (horizontais) e

influências (verticais). Uma análise horizontal, permite perspetivar a possibilidade de preencher/compensar uma lacuna, atuando apenas no mesmo domínio ou, em alternativa, numa ou mais áreas associadas a outros vetores de desenvolvimento da capacidade. Por outro lado, esta visão matricial evidencia também o impacto vertical (influência) destas alterações no conjunto das restantes lacunas, assegurando a sua gestão mais eficiente e eficaz.

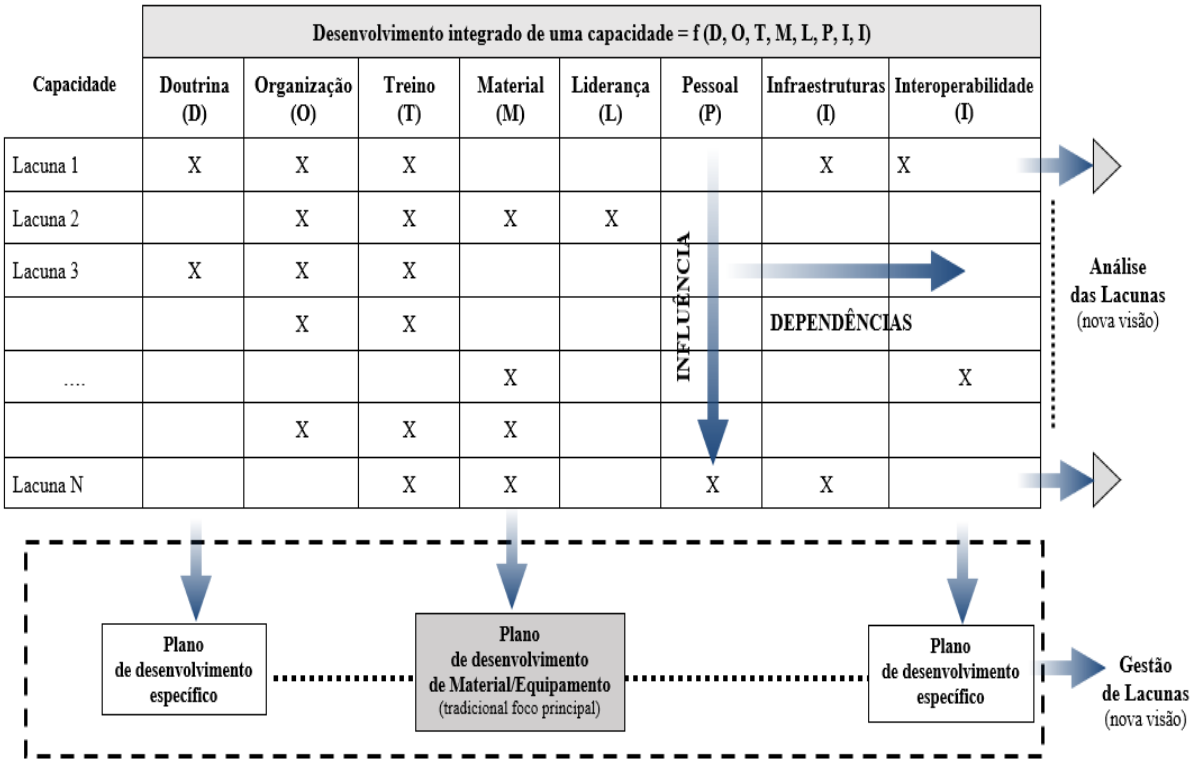


Figura 15 – Modelo de implementação da CCDN

Fonte: Adaptado a partir de Nunes (2015, p.252).

Este tipo de análise, abre também espaço para a criação de planos sectoriais/específicos para cada um dos vetores de desenvolvimento (DOTMLPII) que concorrem para a implementação da capacidade que se pretende edificar. Face à necessidade de garantir uma gestão racional deste processo, muitas vezes caracterizado pela escassez de recursos, a adoção desta metodologia facilitará o estabelecimento criterioso de prioridades, nos vários domínios em que decorre a edificação da CCDN.

Neste aspeto em concreto, atendendo às tendências de evolução da capacidade de ciberdefesa (LE B), a identificação dos programas/projetos de ID&I em curso (LE C), poderá permitir explorar sinergias nacionais e estruturar esforços cooperativos. Conforme se procura demonstrar no apêndice H, o desenvolvimento da CCDFFAA, pode contribuir decisivamente para reforçar a Base Tecnológica e Industrial de Defesa (BTID), tendo um forte impacto noutras áreas tão importantes como o plano de ID&I e o próprio planeamento de DN.

6.4. Cooperação internacional e sinergias nacionais

As áreas de cooperação estratégica no ciberespaço, têm vindo a aprofundar-se através de iniciativas nacionais e internacionais de relevância estratégica, operacional e económica para a edificação de capacidades nacionais.

Nesta matéria, Portugal tem reiteradamente defendido o reforço da cooperação NATO-UE e sublinhado a necessidade da complementaridade das iniciativas a desenvolver, evitando assim a duplicação de esforços (MDN, 2019b). A participação nacional no desenvolvimento da Defesa europeia, nomeadamente em projetos financiados no âmbito PESCO e do FED, tem vindo a potenciar a área da ciberdefesa, promovendo o desenvolvimento de sinergias com a indústria, centros de investigação e universidades.

Portugal tem-se vindo internacionalmente a afirmar como polo de excelência na área da educação, treino e exercícios, nomeadamente, através da liderança do projeto MNCDE&T, da coliderança da *Cyber Defence Discipline* da UE e da instalação da NCI Academy em território nacional. Para este reconhecimento contribui também: a adesão, em 2017, ao *Cooperative Cyber Defence Center of Excellence* (CCDCOE), em Tallinn; a participação em exercícios NATO como o *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise* (CWIX) e o *Cyber Coalition*.

Neste contexto, ao nível da DN, surge como iniciativa agregadora o CAIH, estabelecendo pontes com a área académica e com a BTID, aprofundando a colaboração militar-civil no contexto da segurança do ciberespaço.

No quadro da implementação da ENSC, identificam-se como áreas de cooperação operacional a rede nacional de CSIRT e o G4.

A ligação a empresas, universidades e instituições de ID&I poderá também reforçar a formação de especialistas na área técnica e das CNO, facilitando a constituição de uma "reserva nacional para a ciberdefesa", favorecendo o acesso das FFAA a tecnologias de duplo-uso e a conhecimento de ponta, de forma estruturada e num tempo relativamente reduzido. Em linha com este objetivo, a cooperação internacional no quadro NATO e UE, traz vantagens operacionais acrescidas, nomeadamente, quando for necessário enfrentar um ciberataque de larga escala.

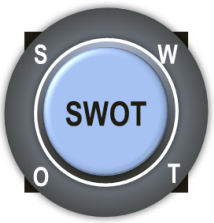
6.5. Avaliação do modelo de edificação da capacidade de ciberdefesa nacional

6.5.1. Análise da situação atual

Face aos objetivos a atingir pelo PDCCD (2019), já em curso, caracterizou-se o nível de maturidade de cada vetor de desenvolvimento e analisou-se o seu impacto na edificação da capacidade. O Apêndice I reflete os resultados obtidos.

6.5.2. Alinhamento estratégico

Complementando a caracterização da situação atual, analisou-se o ambiente envolvente à CCDN (apêndice J), tendo em vista o desenvolvimento de uma análise *Strengths, Weaknesses, Opportunities and Threats* (SWOT). Nesta análise (Figura 16), identificaram-se as Potencialidades (P), Vulnerabilidades (V), Oportunidades (O) e Ameaças (A) mais relevantes.



	Ambiente Interno	
Ambiente Externo	P1 - Doutrina técnico-tática plurissectorial. P2 - Estrutura base para a ciberdefesa edificada. P3 - Mecanismos de fixação dos militares à carreira. P4 - Crescentes oportunidades de treino operacional. P5 - Capacidades identificadas em plataformas tecnológicas edificadas e operacionais. P6 - Comprometimento da estrutura de topo para desenvolver a capacidade. P7 - Financiamento da capacidade assegurado. P8 - Protocolos de cooperação com entidades externas.	V1 - Doutrina - desarticulada ou inexistente. V2 - Estrutura atual não ajustada às necessidades. V3 - Gestão de carreiras e recrutamento. V4 - Educação de base (Academias) e sensibilização. V5 - Parque informático FFAA obsoleto/sem suporte. V6 - Desconhecimento estratégico e falta de integração da capacidade cibernética. V7 - Instalações não comportam aumento RH e áreas técnicas. V8 - Relutância partilha/divulgação vulnerabilidades, comprometimentos, eventos e soluções.
O1 - Doutrina NATO e participação no CCDCOE. O2 - Aproveitamento de sinergias nacionais para melhorar a capacidade de resposta. O3 - Novas tecnologias com aplicação na ciberdefesa (resposta a incidentes - automatização - IA). O4 - Maior visibilidade da segurança do ciberespaço (ENSC)- abertura política para investimento. O5 - Vontade de integração da componente de ciberdefesa das FFAA. O6 - Formação existente em Portugal - Edificação do CAIH (AM) e *NCI Academy* (Oeiras). O7 - Liderança de Projetos internacionais (MNCDE&T e CD Discipline UE). O8 - Partilha de informação com Aliados.	**CRESCIMENTO** **CRIAR** um edifício doutrinário para a ciberdefesa (nível nacional). (P1, P2, P3, P4, P5, P6) X (O1, O2, O4, O5, O8) **PROMOVER** a representação e a cooperação da ciberdefesa nacional. (P4, P6, P7, P8) X (O1, O2, O5, O6, O7, O8) **DINAMIZAR** a evolução futura das soluções tecnológicas para a ciberdefesa. (P1, P5, P6, P7, P8) X (O2, O3, O4, O5, O8)	**FOCALIZAÇÃO** **POTENCIAR** o treino coletivo e individual. (V2, V3, V4) X (O1, O2, O3, O4, O5, O7, O8) **MODERNIZAR** os parques informáticos e as soluções tecnológicas das redes da Defesa. (V5, V7, V8) X (O3, O4, O6) **CONSOLIDAR** infraestruturas e as condições de utilização da capacidade de ciberdefesa. (V5, V7) X (O2, O4, O5)
A1 - Diferentes abordagens doutrinárias. A2 - Compromissos internacionais impõem reforço da capacidade de ciberdefesa. A3 - Utilização crescente do ciberespaço por atores Estado e não-Estado de forma assimétrica. A4 - Formação técnica especializada de duração extensa e custos elevados. A5 - Evolução das ameaças implica uma permanente atualização tecnológica e do conhecimento. A6 - Captação de talentos pela indústria/privados. A7 - Limitada cooperação no combate a ameaças avançadas e persistentes. A8 - Aproximação interagência limitada.	**DIVERSIFICAÇÃO** **PROMOVER** a sensibilização, educação e formação em ciberdefesa (P1, P2, P3, P4, P6, P7, P8) X (A1, A2, A3, A4,A5, A7 , A8) **ADEQUAR** a realidade dos RH afetos à ciberdefesa aos desafios futuros (P1, P2, P3, P4, P6, P7, P8) X (A1, A2, A3, A4, A5, A6, A7) **CONSOLIDAR** processos de interoperabilidade da ciberdefesa com atores externos (P1, P4, P7, P8) X (A1, A2, A7, A8)	**DEFESA** **ADEQUAR** a estrutura da ciberdefesa e a sua integração orgânica face às novas solicitações. (V1, V2, V3, V4, V6, V8) X (A1, A2, A3, A5, A7, A8) **ALINHAR** a resposta genética e operacional e garantir a condução eficiente e eficaz de CNO (V1, V2, V3, V4, V5, V6, V8) X (A1, A2, A3, A5, A7, A8) **ALINHAR** a resposta estrutural e operacional da ciberdefesa nacional face aos desafios futuros. (V1, V2, V3, V4) X (A1, A2, A3, A4, A5, A6, A7, A8)

Figura 16 – Análise SWOT da CCDN

Fonte: Adaptado a partir de EMGFA (2019b).

Como produto da análise SWOT desenvolvida, no Apêndice K, identificam-se 12 Objetivos Estratégicos Estruturantes (OEE) e as correspondentes Linhas de Ação (LA), a desenvolver para assegurar a edificação da CCDN.

6.5.3. Mapa da estratégia militar para o ciberespaço

Seguindo a metodologia estabelecida na DEEMGFA 2018-21, consubstanciando uma resposta às LOENCD, elaborou-se um "mapa da EMCIBER" (Figura 17). Garantiu-se assim o alinhamento dos resultados deste trabalho com as orientações e diretivas estratégicas existentes, incorporando o valor dos esforços já em curso.

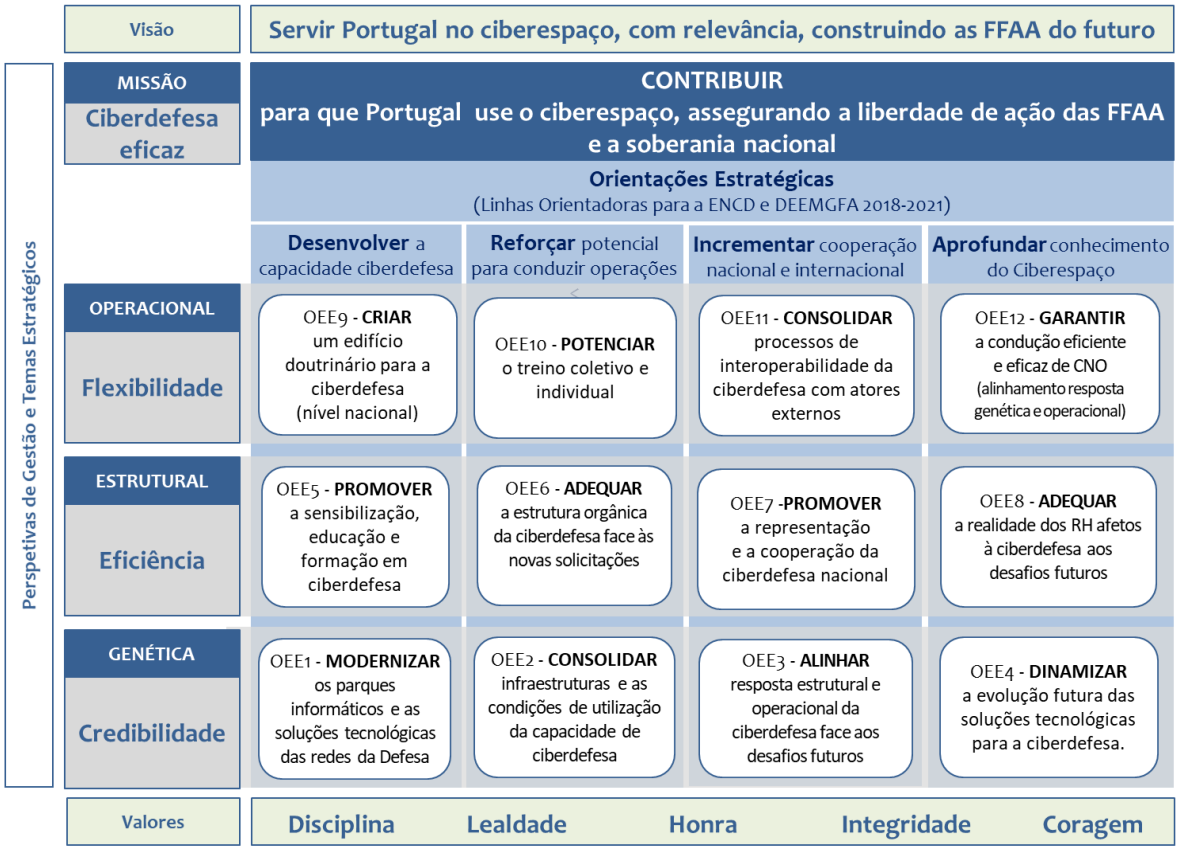


Figura 17 – Mapa da EMCIBER

Fonte: Adaptado a partir de DEEMGFA (2018).

6.5.4. Critérios da avaliação estratégica

Na sequência do exercício de alinhamento estratégico realizado, utilizam-se agora os critérios da adequabilidade, exequibilidade e aceitabilidade para avaliar o modelo proposto.

Na aplicação do critério da adequabilidade, verifica-se que o presente trabalho se encontra alinhado com o CPDM, propõe um processo de gestão integrada de lacunas, estabelece um modelo para o PDCCD, alinhado com a EMCIBER, identifica lacunas/fragilidades decorrentes da análise interna, reconhece as oportunidades e ameaças ao desenvolvimento da CCDN, decorrentes da análise do ambiente externo, e apresenta OEE e LA concretas para responder a estas situações. Desta forma, considera-se que o modelo proposto responde aos objetivos definidos, pelo que se afigura adequado.

Relativamente ao critério da exequibilidade (visão DOTMLPII), encontra-se em preparação um corpo doutrinário, alicerçado na doutrina NATO e dos EUA, tendo sido aprovada uma estrutura transitória, em linha com a nova visão orgânica. A criação de um COCIBER, está prevista ocorrer até 2021. Com algumas limitações, foi, entretanto, preparado um plano de formação e um programa de exercícios. Os requisitos associados às áreas do material/equipamentos e infraestruturas poderão ser satisfeitos, conforme previsto no PDCCD (EMGFA, 2019b), com base no financiamento previsto na última revisão da LPM (2019). Na área do pessoal, subsistem lacunas tanto ao nível do EMGFA como dos Ramos. Neste contexto, preconizam-se medidas específicas, condição essencial para a sustentação desta capacidade prioritária das FFAA. Em linha com a ENSC, o CCD tem vindo a aprofundar a cooperação com as entidades ligadas à ciberdefesa e à cibersegurança nacional, melhorando a sua interoperabilidade funcional e operacional. Deste modo, apesar de se reconhecer o risco associado à carência de RH qualificados e à necessidade de garantir no curto prazo uma capacidade CNO mais robusta e eficaz, afigura-se que o proposto pelo presente modelo é exequível.

Salientando-se o alinhamento do trabalho desenvolvido com as orientações políticas, diretivas estratégicas e planos estabelecidos, considera-se que o modelo proposto satisfaz também o critério da aceitabilidade.

6.6. Plano de Ação

Oferecendo a EMCIBER o quadro estratégico enquadrador da edificação da CCDN, importa converter a visão em ação, atingindo os OEE definidos através da materialização das LA identificadas. Para tal, será necessário monitorizar e controlar a sua execução de forma a facilitar o alinhamento estratégico.

Face às metas estabelecidas, devem assim ser deduzidas métricas e indicadores que permitam avaliar, para cada LA, o grau de concretização dos OEE. Mais do que definir métricas relativas ao que já foi atingido (*log indicators*), importa elencar indicadores "indutores" (*led indicators*), capazes de medir a capacidade de sustentação futura dos resultados (DEEMGFA, 2018, p.39). Este último conjunto de indicadores, influencia normalmente os primeiros, estabelecendo a ligação entre o curto e o longo prazo.

Com base nos OEE a atingir e nos pontos sensíveis/críticos identificados na avaliação estratégica realizada (critério da exequibilidade), será possível revisitar o apêndice K e diferenciar, de forma lógica e coerente as diversas LA, priorizando o que se afirma como mais crítico para a agilização do desenvolvimento da CCDN (OEE: 6, 8, 9 e 12).

A existência de um plano de ação, concretizando a visão estratégica formulada, permitirá realizar a ponte entre o conceito e a ação, reforçando a credibilidade das FFAA, contribuindo decisivamente para dinamizar a edificação da CCDN.

6.7. Síntese conclusiva

Cabe essencialmente à componente genética da EMCIBER a geração e criação dos meios necessários à edificação da CCDN. No entanto, a forma como estes meios são utilizados (visão operacional) e integrados (visão estrutural) influencia substantivamente a edificação desta capacidade.

Com base no modelo de análise, incorporando a visão das entidades entrevistadas, foi possível recolher tendências e confirmar a relevância das variáveis associadas à componente genética da EMCIBER. Na avaliação do nível de maturidade dos vetores de desenvolvimento da capacidade de ciberdefesa, contrastando a situação atual com a desejável, identificaram-se lacunas que importa em tempo colmatar.

Promovendo o alinhamento estratégico do PDCCD no quadro da EMCIBER, realizou-se uma análise SWOT, de onde se derivaram 12 OEE e LA. Este passo, foi complementado com a construção do mapa da EMCIBER e com a avaliação do modelo proposto segundo os critérios da avaliação estratégica (adequabilidade, exequibilidade e aceitabilidade).

Neste contexto, verifica-se que a edificação de um quadro doutrinário, a disponibilidade de RH qualificados, a consolidação das capacidades CNO e o correto posicionamento orgânico da ciberdefesa na estrutura das FFAA são considerados como fatores críticos de sucesso, uma vez que a sua harmonização se revela desafiadora, pelo desfasamento da situação atual relativamente à situação desejável. A definição de um plano de ação, incorporando os resultados desta avaliação, garantirá a monitorização e controlo da execução estratégica, permitindo assegurar o alinhamento com o estado final pretendido.

Em resposta à QD4 (*Qual o modelo de desenvolvimento da CCDFFAA a adotar?*), conclui-se que, conforme determinado pela DMPDM (2019-2022), será adotado um PDCCD das FFAA segundo o modelo DOTMLPII.

Na sua implementação, alinhada e sincronizada com o CPDM nacional, NATO e da UE, devem, sempre que possível, ser exploradas sinergias nacionais e potenciados esforços cooperativos internacionais.

O modelo proposto afigura-se adequado, exequível e aceitável. Estas conclusões, confirmam a H4 levantada.

7. Conclusões

Para Portugal, a informação e a segurança do ciberespaço constituem um vetor estratégico prioritário, não alienável, de afirmação de valores, salvaguarda de interesses e defesa de soberania. Face ao impacto deste novo ambiente operacional na SDN, a construção de uma sociedade digital e a garantia da resiliência operacional das FFAA exige o desenvolvimento de uma EMCIBER, capaz de assegurar uma ciberdefesa credível.

Este TII teve assim como objeto a edificação da CCDN, sendo delimitado nos domínios: temporal, ao período compreendido entre o início do levantamento desta capacidade e o horizonte temporal dos estudos estratégicos analisados; espacial, ao conjunto de decisores militares e civis que, direta ou indiretamente, influenciam o desenvolvimento da CCDN; e de conteúdo, ao domínio da EMCIBER, de onde deriva esta capacidade.

Neste âmbito, norteou-se pela QC de investigação: *Qual o modelo a adotar para a edificação da CCDFFAA, de forma a dinamizar a edificação da CCDN, e a dotar as FFAA com uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço?*

No que concerne ao procedimento metodológico, esta investigação desenvolveu-se em três fases (exploratória, analítica e conclusiva), seguindo um raciocínio hipotético-dedutivo, assente numa estratégia de investigação essencialmente qualitativa e num desenho de estudo de caso.

No que à estrutura diz respeito, o TII ancora sete capítulos: introdução, enquadramento teórico e conceptual (com a revisão da literatura, metodologia e método), análise do impacto estratégico do ciberespaço e definição de uma EMCIBER, caracterização das suas componentes operacional, estrutural e genética, de onde decorre a edificação da CCDN, e conclusões.

Relativamente aos objetivos desta investigação, no que se refere ao OE1 (*Propor, face ao impacto estratégico do ambiente da informação, a definição de uma EMCIBER)*, concretizado através da resposta à QD1, este foi satisfeito através da revisão bibliográfica, análise documental e da realização de uma entrevista a decisores ligados à ciberdefesa das FFAA e à cibersegurança nacional. A partir da análise de conteúdo das entrevistas realizadas, foi possível recolher tendências relativamente aos elementos (âmbito e finalidade) e componentes caracterizadoras da EMCIBER (operacional, estrutural e genética), sendo apresentada a sua definição. Tal confirmou a H1 formulada.

A concretização do OE2 (*Analisar, ao nível da estratégia operacional, o impacto do reconhecimento nacional do ciberespaço como quarto domínio das operações)*, decorrendo da resposta à QD2, foi também materializada através da análise documental da doutrina NATO e da

recolha da perceção dos entrevistados relativamente à maturidade doutrinária nacional, relevante para apoiar um conceito de emprego de forças. Confirmando a natureza das implicações operacionais do reconhecimento do ciberespaço como novo domínio das operações, seguindo uma lógica multi-domínio, a generalidade dos responsáveis pela ciberdefesa nacional considera o ciberespaço fundamental para a realização de qualquer tipo de operação militar, independentemente da conjuntura e/ou situação. Neste contexto, as OpCiber devem ser planeadas ao nível estratégico-operacional e executadas ao nível operacional e tático/técnico, envolvendo a condução de operações defensivas e ofensivas. Confirmou-se assim a H2 levantada.

Tendo por foco o OE3 (*Analisar os constrangimentos dos RH das FFAA e os diferentes modelos orgânicos existentes, de forma a promover o levantamento da estrutura nacional de ciberdefesa*), promoveu-se a sua consecução através da resposta à QD3. Para esse efeito, analisou-se num primeiro passo a organização existente em diversos países aliados, identificando princípios comuns, passíveis de aplicação à realidade nacional. Com base na situação atual, conforme percebida, desenhou-se uma resposta estrutural para a EMCIBER, alinhada com a visão operacional antes definida: Comando conjunto e autónomo, na dependência direta do CEMGFA, incluindo militares e civis. De forma a facilitar a coordenação político-estratégica da ciberdefesa em situações de crise, propôs-se também a criação do CSDC. Reconhecendo-se a existência de constrangimentos ao nível dos RH das FFAA, condicionadores da eficácia das capacidades CNO, foram identificadas medidas concretas, destinadas a colmatar as fragilidades existentes, ao nível da gestão de carreiras, desenvolvimento de competências/conhecimento especializado, recrutamento e retenção de quadros qualificados. Entre as medidas elencadas, salienta-se a proposta de criação de um quadro especial para pessoal afeto à ciberdefesa, o desenvolvimento de protocolos para o reforço das capacidades CNO e a constituição de uma reserva nacional de ciberdefesa, permitindo potenciar sinergias nacionais (*e.g.*, ID&I, indústria e academia), garantir uma maior capacidade de resposta e reforçar a resiliência nacional. Foi assim confirmada a H3.

O OE4 (*Analisar o modelo de desenvolvimento da capacidade de ciberdefesa das FFAA*), foi concretizado através da resposta à QD4. Para esse efeito, foram analisados o PDC e a gestão integrada de lacunas, associados ao CPDM nacional, NATO e da UE. Com base neste enquadramento, validado pela perceção recolhida dos entrevistados, foi definido um PDCCD, seguindo um modelo baseado no desenvolvimento integrado dos vetores da CCDFFAA. Em linha com a ENSC, este processo deverá ser articulado com os esforços em curso na área da cibersegurança, explorando sinergias nacionais e a cooperação internacional,

dinamizando assim a edificação da CCDN. Resulta assim também confirmada a H4.

Como corolário da investigação, relativamente ao OG (*Avaliar o processo de desenvolvimento da CCDFFAA, de forma a dinamizar a edificação da CCDN, e a dotar as FFAA com uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço*), em resposta à QC que dele decorre, o processo de desenvolvimento da CCDN foi avaliado quanto ao grau de consecução dos objetivos traçados para cada um dos vetores de capacidade, ao seu alinhamento e à verificação dos critérios da avaliação estratégica (adequabilidade, exequibilidade e aceitabilidade). Facilitando a implementação da EMCIBER, o modelo proposto consolida o processo de edificação da CCDFFAA, estimula o desenvolvimento de sinergias nacionais e a cooperação internacional. Desta forma, responde aos objetivos definidos, pelo que se considera adequado. Apesar dos riscos identificados, não negligenciáveis, afigura-se que o proposto por este modelo é exequível. Refletindo este estudo o alinhamento com as orientações políticas, diretivas estratégicas e planos estabelecidos, o critério da aceitabilidade foi igualmente satisfeito.

Decorrendo da avaliação realizada e do plano de ação delineado para assegurar o alinhamento da execução estratégica, ancorado na consecução dos OE definidos, considera-se o OG desta investigação atingido.

Tem-se, assim, como **principais contributos para o conhecimento** a definição de uma EMCIBER e de um processo integrado de desenvolvimento da CCDFFAA, alinhado com as suas componentes estruturantes. Preenchendo um hiato existente na articulação da estratégia militar do País, a EMCIBER, conforme definida nas suas vertentes operacional, estrutural e genética, oferece o enquadramento conceptual necessário para dinamizar a edificação da CCDN. Neste âmbito, os resultados deste estudo constituem também um contributo para os esforços de desenvolvimento da ENCD, ainda em curso.

Como possível **limitação da investigação** elenca-se o facto de o tratamento do tema ter exigido a contextualização prévia do objeto de estudo. De forma a contrariar o risco de enviesamento, o percurso metodológico foi sustentado em documentos de referência e nas perceções dos especialistas entrevistados.

No que concerne a **estudos futuros**, afigura-se interessante aplicar os resultados desta investigação, a título de subsídio, aos trabalhos de definição da ENCD e na futura revisão do CEM, nomeadamente, pelas suas implicações diretas na conceptualização da EMCIBER. Complementando esta investigação, apresenta-se ainda como importante a formulação de um

plano de ação mais detalhado para a EMCIBER, permitindo fazer face a eventuais desvios ou alterações conjunturais imprevistas da sua implementação. Promovendo uma contextualização estratégica mais alargada, considera-se também uma mais-valia estudar o impacto da EMCIBER nas restantes áreas da Estratégia Militar.

A principal **recomendação de ordem prática** que decorre deste trabalho, prende-se com a necessidade de criar e operacionalizar, com a maior brevidade possível, uma EMCIBER. Tal constitui um imperativo para as FFAA, nomeadamente, porque se torna necessário preencher as lacunas existentes no edifício da estratégia nacional que, neste momento, ainda não contextualiza com a devida propriedade a dimensão cibernética dos conflitos na sua estratégia militar. Sem uma EMCIBER credível, o desenvolvimento da CCDN corre o risco de não refletir o seu desígnio.

Reconhecendo que as FFAA contribuem de forma cooperativa e supletiva para a segurança do ciberespaço, intervindo ativamente nos seis eixos de atuação da ENSC, recomenda-se também a criação de um sétimo eixo no plano de ação desta estratégia, designado por "salvaguarda da soberania nacional no ciberespaço", de forma a melhor traduzir o papel específico da DN neste domínio.

Atendendo às opções estratégicas a assumir no curto-prazo, salvo melhor opinião, considera-se relevante seguir as melhores práticas, já consolidadas e adotadas por outros Países, impondo-se uma alteração da atual cultura e paradigma operacional.

De forma realista, olhar o futuro é a melhor forma de inspirar a transformação do presente.

Referências Bibliográficas

AJP-3.10. (2009). *Allied Joint Doctrine for Information Operations*. Bruxelas: NATO Standardization Office.

AJP-3.20. (2020). *Allied Joint Doctrine for Cyberspace Operations (Edition A), Version 1*. Bruxelas: NATO Standardization Office.

AJP-5.0 (2019). *Allied Joint Doctrine for the Planning of Operations (Edition A)*. Bruxelas: NATO Standardization Office.

Alves. J. L. (1998). *Estratégia – Panorama Geral e sua Teoria*. Lisboa: Publicações Dom Quixote.

Beaufre, A. (1965). *Introduction a la Stratégie*. Paris: Librarie Armand Colin.

Brangetto, P. (2015). *National Cyber Security Organisation: France*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Bryman. (2012). *Social Research Methods* (4.ª Ed.). New York: Oxford University Press.

Capability Development Mechanism. (2003). *Capability Development Mechanism* (documento doutrinário reservado). Bruxelas: European Defense Agency.

Capability Development Plan. (2018). Capability Development Plan (CDP) - Fact sheet da European Defence Agency [Página *online*]. Retirado de https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f.

Cendoya, A. (2016). *National Cyber Security Organisation: Spain*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Centro de Investigação e Desenvolvimento do Instituto Universitário Militar. (2018). Domínios, Áreas e Subáreas de Investigação [Página *online*]. Retirado de https://cidium.ium.pt/site/index.php/pt/investiga/dominios-areas-e-subareas-de-investigacao.

Clausewitz. C. V. (1976). *Da Guerra*. Lisboa: Publicações Perspetivas e Realidades.

Conselho Superior de Defesa Nacional (2014). *Conceito Estratégico Militar*. Retirado de https://www.fd.unl.pt/docentes_docs/ma/FPG_MA_27255.pdf.

Convenção de Genebra. (1949). Direito Humanitário Internacional: Convenção de Genebra [Página *online*]. Retirado de: http://www.mpsp.mp.br/portal/page/portal/cao_civel/normativa_internacional/Sistema_ONU/DH.pdf, em 03 de maio de 2020.

Couto, A. C. (1988). *Elementos de Estratégia - Volume I*. Lisboa: Instituto de Altos Estudos Militares.

Decreto-Lei n.º 69/2014, de 09 de maio (2014). *Cria o Centro Nacional de Cibersegurança (CNCS)*. Diário da República, 1.ª Série, 89, 2712-2719. Lisboa: Presidência do Conselho de Ministros.

Estado-Maior do Exército. (2015). *Relatório Final do Exercício "Ciber Perseu 2014"* (Relatório). Lisboa: Direção de Comunicações e Sistemas de Informação.

Estado-Maior do Exército. (2018). *Relatório Final do Exercício "Ciber Perseu 2018"* (Relatório). Lisboa: Direção de Comunicações e Sistemas de Informação.

Estado-Maior-General das Forças Armadas. (2018). *Diretiva Estratégica do EMGFA 2018-2021*, de 18 abril de 2018. Lisboa: Chefe do Estado-Maior-General das Forças Armadas.

Estado-Maior-General das Forças Armadas. (2019a). *Proposta de Estratégia Nacional para a Ciberdefesa 2019-2023*. Lisboa: Grupo de Trabalho-Capacidade Ciberdefesa das FFAA.

Estado-Maior-General das Forças Armadas. (2019b). *Relatório do Estudo de Desenvolvimento da Capacidade de Ciberdefesa*. Lisboa: Grupo de Trabalho-Capacidade Ciberdefesa das FFAA.

Estado-Maior-General das Forças Armadas. (2020). *Ciberdefesa – Ponto de Situação* (Ofício N.º 0164/GC-S). Lisboa: Gabinete do CEMGFA.

Fox, A. (2017, janeiro-março). Looking Toward the Future: The U.S. Cavalry´s Role in Multi-Domain Battle. *Cavalry and Armor Journal*, 29-36.

Freixo, M.J.V. (2011). *Metodologia Científica: Fundamentos, Métodos e Técnicas* (3.ª Ed.). Lisboa: Instituto Piaget.

Hill, M. & Hill, A. (2002). Investigação por questionário (2.ª Ed.). Lisboa: Sílabo.

Hoffmann, R. (2019, março). German Cyber and Information Domain Service – German Perspective on Cyber Operations, *NATO Information Assurance Symposium*. Simpósio organizado pela NATO Communications and Information Agency, Mons.

ITA-CS (2017). *The Italian Cybersecurity Action Plan*. Rome: Presidency of the Council of Ministers.

Lei Orgânica n.º 02/2019, de 17 de junho (2019). *Aprova a Lei de Programação Militar* (LPM) e revoga a Lei Orgânica n.º 7/2015. Diário da República, 1.ª Série, 114, 2982-2985. Lisboa: Assembleia da República.

Lei Orgânica n.º 46/2018, de 13 de agosto (2018). *Aprova o Regime Jurídico da Segurança do Ciberespaço*. Diário da República, 1.ª Série-A, 155, 4031-4037. Lisboa: Assembleia da República.

Maroco, J. (2003). Análise Estatística com utilização do SPSS. Lisboa: Edições Sílabo.

McChrystal, S. (2015). *Team of Teams: New Rules of Engagement for a Complex World*. Nova Iorque: Portfolio/Penguin.

Ministério da Defesa Nacional. (2013). *Orientação para a Política de Ciberdefesa* (Despacho n.º 13692/MDN, de 11 de outubro). Lisboa: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2018). *Diretiva Ministerial de Orientação Política para o Investimento na Defesa* (Despacho n.º 4103/MDN, de 12 de abril). Lisboa: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2019a). *Proposta de Estratégia Nacional de Ciberdefesa* Lisboa: Direção-Geral de Recursos da Defesa Nacional.

Ministério da Defesa Nacional. (2019b). *Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa-Horizonte 2019-23* (Despacho n.º 52/MDN, de 23 de outubro). Lisboa: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2020a). *Diretiva Ministerial de Planeamento de Defesa Militar* (Despacho n.º 2536/MDN, de 24 de fevereiro). Lisboa: Ministro da Defesa Nacional.

Ministério da Defesa Nacional. (2020b). *Criação do Comité de Monitorização da Ciberdefesa* (Despacho n.º 15/2020, de 06 de fevereiro). Lisboa: Ministro da Defesa Nacional.

NATO Defence Planning Process. (2020). North Atlantic Treaty Organization [Página *online*]. Retirado de, https://www.nato.int/cps/en/natohq/topics_49202.h0.

NLD-MOD. (2018). *Defense Cyber Strategy 2018: Investing in a digital military capability*. Holanda: Dutch Ministery of Defense.

North Atlantic Treaty Organization. (2010). NATO Strategic Concept 2010 [Página *online*]. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf, em 14 de maio de 2020.

North Atlantic Treaty Organization. (2013). *Comprehensive Operations Planning Directive* (Diretiva). Mons: Strategic Allied Command Operations.

North Atlantic Treaty Organization. (2014a). *Walles Summit Declaration Press Release* 2014-120 [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en.

North Atlantic Treaty Organization. (2014b). *Enhanced NATO Policy on Cyber Defence* (Decisão PO/2014/0358). Bruxelas: Emergency Security Challenge Division.

North Atlantic Treaty Organization. (2016a). *Cyber Defence Pledge*. NATO Warsaw Summit Press Release (Comunicado 124). Bruxelas: NATO Allied Council.

North Atlantic Treaty Organization. (2016b). *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations,* (Diretiva MC0593/1). Bruxelas: Military Committee.

North Atlantic Treaty Organization. (2017). *Approval of the Roadmap to implement Cyberspace as a Domain of Operations* (Decisão PO/2017/0072-INV). Bruxelas: NATO Allied Council.

North Atlantic Treaty Organization. (2018a). Brussels Summit Declaration Press Release 2018-074 [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

North Atlantic Treaty Organization. (2018b). *Military Vision and Strategy on Cyberspace as a Domain of Operations* (Decisão de 12 de junho). Bruxelas: Military Committee.

North Atlantic Treaty Organization. (2018c). *High Level Taxonomy of Cyberspace Operations* (Taxonomia IMSM-0222-2018). Bruxelas: NATO International Military Staff.

North Atlantic Treaty Organization. (2019a). London Declaration Press Release [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_171584.htm.

North Atlantic Treaty Organization. (2019b). NATO Cyber Defence [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm.

North Atlantic Treaty Organization. (2019c). *Cyberspace Domain C2 CONOPS* (Guia de Planeamento). Mons: Strategic Allied Command Operations.

North Atlantic Treaty Organization. (2019d). *Cyberspace Operations Functional Planning Guide* (Guia de Planeamento). Mons: Strategic Allied Command Operations.

North Atlantic Treaty Organization. (2019e). *NATO Crisis Response System Manual* (Manual). Bruxelas: Military Committee.

Nunes, P. V. (2004). *A conflitualidade da informação: da guerra de informação à estratégia da informação* (Trabalho de Investigação Individual do Curso de Estado Maior). Instituto de Altos Estudos Militares, Lisboa.

Nunes, P. V. (2010). *Análise da Conflitualidade da Informação na Sociedade em Rede: Um enquadramento para a conceção e implementação de um modelo de Estratégia da Informação Nacional* (Tese de Doutoramento em Ciências da Informação). Universidade Complutense [UC], Madrid.

Nunes, P. V. (2015). *Sociedade em Rede, Ciberespaço e Guerra de Informação - contributos para o enquadramento e construção de uma Estratégia Nacional da Informação* (2.ª Ed.). Lisboa: Instituto da Defesa Nacional.

Nunes, P. V. (Coord.). (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa.* IDN Cadernos, 28. Lisboa: Instituto da Defesa Nacional.

Organização das Nações Unidas (1945). Carta das Nações Unidas [Página *online*]. Retirado de http://oas.org/dil/port/1945%20Carta%20das%20Nações%20Unidas.pdf, em 03 de maio de 2020.

Osula, A. (2015). *National Cyber Security Organisation: United Kingdom*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Pernik, P. & Verschoor-Kirss, A. (2016). *National Cyber Security Organisation: United States*. Tallinn: Cooperative Cyber Defence Centre of Excellence.

Pires, N. (2018). *O Conceito Multi-Domínio e as Possíveis Aplicações às Forças Armadas Portuguesas*. Coleção ARES, 24. Lisboa: Instituto Universitário Militar.

Quivy, R. & Campenhoudt, L. (2003). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.

Ramalho. P. (2000). A crise internacional – a sua Gestão. *Revista Estratégia- volume XII*. Lisboa: Editorial Presença.

Resolução da Assembleia da República n.º 15/2005, de 07 de abril. (2005). *Aprova a VII Revisão Constitucional da Constituição aprovada pela Assembleia Constituinte, 02 de abril de 1976*. Diário da República, 1.ª Série, 74, 2979-2979. Lisboa: Assembleia da República.

Resolução do Conselho de Ministros n.º 115/2017, de 13 de julho de 2017. (2017). *Cria o grupo de projeto denominado "Conselho Superior de Segurança do Ciberespaço"*. Diário da República, 1.ª Série, 163/2017, 5035 – 5037. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª Série, 67, 1981–1995. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril. (2013). Aprova a reforma "Defesa 2020". Diário da República, 1.ª Série, 77, 2285–2289. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 92/2019, de 05 de junho. (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1ª Série, 108, 2888–2895. Lisboa: Presidência do Conselho de Ministros.

Santos, L.A.B., & Lima, J.M.M (Coord.). (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.ª Ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

SAS-143. (2019). *Agile Multi-Domain C2/Harmonization*. *Systems Analysis and Simulation Group N. º 143* (draft Relatório Final). Paris: Research and Technology Organization.

Schmitt, M. N. (Coord.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

União Europeia -North Atlantic Treaty Organisation. (2016). Statement on the implementation of the Joint EU-NATO Declaration [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

União Europeia. (2009). *EU Concept for Computer Network Operations in EU-led Military Operations* (Decisão EEAS13537/09). Bruxelas: European Union Military Staff.

União Europeia. (2012). *EU Concept for Cyber Defence for EU-led Military Operations* (Decisão EEAS01729/12). Bruxelas: European Council.

União Europeia. (2016). *Implementação da Declaração Conjunta EU-NATO – conjunto de propostas comuns* (Conclusões do Conselho 15283/16). Bruxelas: European Council.

Wieriks, S. (2018). *Cyber Operations integration in the operational planning process.* Holanda: NLD Defense Cyber Command.

Apêndice A — Corpo de conceitos

Ambiente da informação – "O espaço físico e virtual em que a informação é recebida, processada e partilhada. Consiste nos sistemas de informação e na própria informação" (AJP-3.10, 2009, p. Lex-6). Conceptualmente, considera-se que o ambiente da informação é algo maior do que o próprio ciberespaço (de natureza digital) pois inclui a informação em formato digital e não digital.

Capacidade militar – **"**aptidão requerida a uma força ou organização militar para que possa cumprir determinada tarefa ou missão" (CSDN, 2014, p.38). No âmbito do processo de desenvolvimento e melhoria de capacidades NATO, são considerados diversos vetores de desenvolvimento, como sejam a Doutrina, Organização, Treino, Material, Liderança, Pessoal, Instalações e Interoperabilidade (DOTMLPII).

Ciberdefesa – consiste na "atividade que visa assegurar a Defesa Nacional no, ou através do, ciberespaço" (ENSC, 2019). Traduz também o conjunto de atividades e meios "através dos quais se atingem e executam medidas defensivas para fazer face a ciberataques e mitigar os seus efeitos, preservando e restaurando assim a segurança do ciberespaço e permitindo assegurar a garantia da missão (*mission assurance*)" (NATO, 2018c, p.A-1).

Cibersegurança – consiste no "conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" (RCM n.º 92/2019, de 05 junho).

Ciclo de desenvolvimento de capacidades – processo cíclico associado ao desenvolvimento de capacidades que, partindo do nível de ambição estratégica e com base na identificação das necessidades daí decorrentes, permite determinar a existência de eventuais lacunas, avaliar o seu impacto e promover o seu preenchimento de forma a reduzir o risco operacional por elas originado (CDP, 2018).

Defesa Nacional – "constitui uma estratégia integrada que o Estado põe em prática para garantir uma situação de "segurança" nacional. A Defesa Nacional inclui essencialmente duas componentes: uma de natureza militar e outra de natureza não militar. A defesa militar, consubstancia essencialmente a defesa contra-ameaças externas e agressões armadas. Por outro lado, a defesa civil (não militar), apresenta uma natureza mais ampla, abrangendo áreas como a proteção civil, a segurança interna, a defesa económica, social e cultural do País" (Ramalho, 2000, p.171-172).

Estratégia – é "a ciência e a arte de desenvolver e utilizar as forças morais e materiais de uma unidade política ou coligação, a fim de se atingirem objetivos políticos que suscitam, ou podem suscitar, a hostilidade de uma outra vontade política" (Couto, 1988, p.209).

Estratégia operacional – "trata da conceção e execução da manobra estratégica nos vários domínios, competindo-lhe conciliar o objetivo a atingir com as possibilidades permitidas pela organização, pelas táticas e técnicas do domínio considerado, mas também orientar a evolução daquelas de forma a adaptá-las às necessidades da estratégia" (Couto, 1988, p.231).

Estratégia estrutural – "tem por objeto, em todos os domínios, o estudo e análise das estruturas existentes, identificando as suas vulnerabilidades e as suas potencialidades, tendo em vista a determinação das medidas mais adequadas para reforçar as suas possibilidades e atenuar as suas lacunas, conduzindo a um melhor rendimento dos meios e recursos" (Couto, 1988, p.232).

Estratégia genética – "visa pôr à disposição dos diversos sectores e áreas da estratégia operacional os meios necessários para a sua consecução, no momento adequado, de forma a que suportem o conceito estratégico adotado. O nível de ambição da estratégia operacional, deverá assim ser identificado de forma realista, atendendo à disponibilidade dos meios necessários" (Couto, 1988, p.231- 232).

Estratégia militar – constituindo uma das componentes da estratégia total e a esta subordinada, enquanto estratégia geral, a estratégia militar pode ser definida como "a ciência e arte de desenvolver as Forças Armadas com vista à consecução de objetivos fixados pela Política" (Couto, 1988, p.229). A responsabilidade pela condução da estratégia militar é do Ministro da Defesa Nacional.

Garantia da informação (*Information Assurance*) – salientando uma "postura defensiva relativamente à defesa da informação e dos sistemas de informação e comunicação, compreende todos os aspetos relacionados com a proteção, verificação e garantia da disponibilidade da informação e dos sistemas que armazenam, processam e transportam essa informação" (NATO, 2018b, p.A-1).

Garantia da missão (*Mission Assurance*) – constitui um "processo destinado a garantir a proteção ou a assegurar o funcionamento contínuo e a resiliência de capacidades e recursos, incluindo pessoal, equipamento, instalações, redes, informação e sistemas de informação, infraestruturas e cadeias de abastecimentos, críticas para a execução das funções essenciais para o cumprimento da missão em qualquer condição ou ambiente operacional. Evidencia o impacto operacional da ocorrência de incidentes e ataques no ciberespaço" (NATO, 2018c, p.A-1).

Informação – "é um conjunto de dados em contexto, cuja forma e conteúdo são apropriados para uma aplicação particular, a partir dos quais é possível conhecer um determinado aspeto ou parte da realidade" (Nunes, 2015, p.34).

Operações em redes de computadores (*Computer Network Operations*) – são "ações conduzidas em redes de computadores e no ambiente de informação para produzir efeitos em redes e computadores" (AJP-3.10, 2009, p.2A-6). "A oportunidade e eficácia das *Computer Network Operations* (CNO) é proporcional à dependência do adversário relativamente às tecnologias da informação. As CNO integram três elementos: *Computer Network Attack* (CNA), *Computer Network Exploitation* (CNE) e *Computer Network Defense* (CND)" (AJP-3.10, 2009, p.1-11).

Operações defensivas no ciberespaço – são "ações defensivas desenvolvidas no e através do ciberespaço para preservar a liberdade de ação das forças amigas" (NATO, 2018c, p. A-2-3).

Operações multi-domínio – consistem no "conjunto de operações em que se encontram envolvidas entidades ou atores que operam e/ou geram efeitos em mais do que um domínio" (SAS-143, 2019).

Operações no ciberespaço – consistem no "conjunto de ações desenvolvidas no e através do ciberespaço, com a intenção de preservar a liberdade de ação das forças amigas e/ou criar efeitos no ciberespaço para atingir os objetivos definidos pelo comandante" (NATO, 2018c, p. A-2-1).

Operações ofensivas no ciberespaço – são "atividades desenvolvidas no e através do ciberespaço para projetar poder e gerar efeitos destinados a atingir objetivos operacionais" (NATO, 2018c, p. A-2-5).

Redes da Defesa Nacional – são as redes e SIC do Ministério da Defesa Nacional, Secretaria Geral, Centro de Dados da Defesa, Ramos das FFAA e EMGFA.

Segurança da informação – é o conjunto de atividades destinadas a "assegurar a proteção da informação (armazenada, processada ou transmitida), assim como dos sistemas de armazenamento, contra a perda de confidencialidade, integridade e disponibilidade, através da adoção de diversas medidas de controlo de natureza procedimental, técnica ou administrativa" (AJP-3.10, 2009, p. Lex-6).

Apêndice B — *Focus group* e questionário exploratório

1. Enquadramento e estabelecimento do *focus group*

Atendendo aos objetivos deste estudo, considerou-se importante recolher numa fase inicial da investigação dados da realidade a estudar. Neste âmbito, foram realizadas diversas conversas/entrevistas preliminares com reconhecidos especialistas nacionais e internacionais de forma a recolher tendências, obter uma maior sensibilidade para a abordagem do tema e avaliar a coerência das hipóteses levantadas.

Neste âmbito, foram também tidos em consideração os resultados de um questionário utilizado no âmbito de um trabalho de investigação, subordinado ao tema "A conflitualidade da informação: da guerra de informação à estratégia da informação" (Nunes, 2004), onde se procurou analisar o impacto da utilização da informação na atividade das FFAA, evidenciando as suas implicações ao nível estratégico e operacional. Neste questionário, o processo de amostragem, não teve por base uma amostra aleatória e consequentemente não manteve a proporcionalidade em relação ao universo estudado[5]. No entanto, apesar disso, permitiu recolher tendências e obter dados importantes relativamente a alguns dos indicadores e variáveis do presente estudo.

De forma a promover a revisão, atualização e validação das conclusões deste estudo, foi estabelecido um *focus group* com base nos auditores do 3.º CPOCIBER. Este grupo, composto por 21 Oficiais (Marinha, Exército, Força Aérea e Guarda Nacional Republicana), com o posto de Capitão a Tenente-Coronel, reunindo conhecimento específico na área da segurança da informação e da ciberdefesa, constitui uma amostra empírica, válida e representativa da realidade a estudar.

Aproveitando esta oportunidade, procurou-se também testar a coerência de algumas das questões a incluir no guião da entrevista realizada no âmbito deste TII. Com esse intuito, foi aplicado a todos os participantes um questionário com duas questões múltiplas de avaliação (Santos & Lima, 2019, p.79), relacionadas com o nível de maturidade doutrinária e o nível de integração operacional de capacidades de ciberdefesa. Foi assim possível obter sugestões/observações pertinentes que motivaram a realização de alterações pontuais no guião da entrevista.

Após o preenchimento deste questionário, foi efetuada a sua codificação e compilados os dados recolhidos, realizando uma análise estatística do tipo descritivo. Foram depois determinadas as médias e frequências de cada categoria para as variáveis em análise. Os questionários preenchidos, encontram-se nos arquivos do autor do presente TII.

A reunião do *focus group* decorreu no dia 12 de dezembro de 2019, nas instalações do IUM.

2. Metodologia seguida

A condução dos trabalhos do *focus group* decorreu ao longo de quatro fases: i) preparação e apresentação de dados; ii) contextualização; iii) discussão; iv) síntese e conclusões.

A primeira fase, antecedendo a reunião plenária do *focus group*, envolveu a análise dos resultados obtidos no estudo anterior (Nunes, 2010, pp. 357-369) e a sua compilação numa apresentação, destinada a sistematizar e facilitar a sua posterior discussão. A fase da contextualização, tendo lugar no início da reunião, permitiu clarificar o objetivo do *focus group*, os princípios utilizados na construção do estudo a analisar, o seu enquadramento no contexto deste TII, e as várias fases da condução dos trabalhos.

[5] A amostra foi constituída por 72 pessoas que desempenhavam cargos de direção e gestão de áreas funcionais de organizações militares e civis. No contexto militar, a amostra integrou Oficiais do Quadro Permanente dos três Ramos das FFAA, com o posto de Coronel/Capitão de Mar-e-Guerra ou Major/Capitão-Tenente.

Na fase da discussão, foram apresentadas e discutidas sequencialmente as perceções formuladas com base nas respostas a cada grupo de questões, contidas no questionário em análise. Neste contexto, foram recolhidas as observações/comentários formulados pelos participantes. Num último passo, foram sintetizados, revistos e integrados todos os comentários recebidos na síntese conclusiva que a seguir se apresenta.

3. Síntese conclusiva

Com base nos resultados da discussão do *focus group*, na análise dos contributos recebidos e após a sua síntese, foram recolhidas as perceções que a seguir se apresentam.

A rede é a base de funcionamento da organização, sendo considerada respetivamente como muito elevada e elevada a sua importância e o nível de dependência gerada relativamente ao seu funcionamento correto. Considera-se como importante ou muito importante o acesso à internet e a utilização dos sistemas de informação, assumindo estes uma importância acrescida no funcionamento das atividades primárias da organização e na tomada de decisão ao nível da gestão de topo e intermédia.

As quebras de segurança são consideradas como uma das ameaças à utilização da informação no âmbito estratégico e operacional da organização, sendo a segurança reduzida face às ameaças que se colocam aos SIC e à exploração das redes das FFAA. As violações de segurança da informação afetam fundamentalmente a disponibilidade dos recursos, sendo considerados os ataques de *software* malicioso como a principal e mais perigosa ameaça externa (forma de ataque) e a nível interno a má preparação técnica dos utilizadores da rede. **Deste modo, face à utilização conflitual da informação, foi possível reforçar a perceção para a necessidade imperiosa de existir uma política de segurança da informação que, ao nível operacional, garanta a implementação de mecanismos específicos de proteção e segurança das redes das FFAA**.

Face à perceção dos decisores para a má preparação técnica dos utilizadores, verifica-se existirem necessidades de formação que devem ser colmatadas. Neste contexto, sai reforçado o desempenho de funções de acordo com o perfil de competências do colaborador. Face ao desconhecimento técnico relativamente à utilização de *software*, é reconhecido que alguns utilizadores podem inadvertidamente pôr em risco a segurança da informação e a própria organização. De salientar o facto desta situação poder vir a configurar as condições necessárias para o lançamento de ataques de engenharia social, explorando a dimensão humana de forma a atingir a dimensão aplicacional dos SIC e a capacidade operacional da organização. Neste contexto, **sendo estabelecida uma estrutura dedicada à ciberdefesa, importa garantir o alinhamento organizacional, de acordo com o perfil de competências dos quadros existentes, para fazer face à necessidade de as FFAA disporem de RH qualificados neste domínio**. Devem ser também reforçadas as ações de sensibilização para a cibersegurança nas FFAA e no âmbito da Defesa. **Devido à possível ocorrência de ciberataques, devem ser levantadas ações defensivas, nomeadamente, destinadas a reforçar a proteção e segurança das redes das FFAA e da Defesa. O parque informático e as ferramentas de segurança da informação devem ser continuamente atualizados**. **Afirma-se assim a perceção da necessidade de estabelecer uma estratégia para o ciberespaço/ambiente da informação nas suas vertentes operacional, estrutural e genética.**

Em conclusão, este inquérito exploratório permitiu validar a pertinência da formulação da QC e QD, evidenciando também a coerência das hipóteses que a estas se encontram associadas. Adicionalmente, a análise das conclusões recolhidas do *focus group* ofereceu importantes indicadores que se procurarão explorar ao longo deste estudo.

Apêndice C — Análise estatística dos dados (questionário e entrevista)

1. Enquadramento

Este apêndice sintetiza a análise estatística dos dados recolhidos a partir da aplicação de um questionário aos 21 auditores do 3.º CPOCIBER. As duas questões formuladas (fechadas de avaliação), foram também incluídas no guião da entrevista (Questão 3. e 5.) realizada a doze especialistas, conforme se apresenta no Apêndice D.

A análise quantitativa dos dados recolhidos foi efetuada de forma agregada, com recurso ao *Statistical Package for the Social Sciences* (SPSS 23.0) e ao *IBM SPSS AMOS* (versão 23), conforme aqui se apresenta.

Neste âmbito, para além da estatística descritiva (*e.g.*, média, desvio padrão, entre outras), foram estimados: coeficientes de correlação, utilizando o *"r* de *Pearson"* (Hill & Hill, 2002, p.219), a consistência interna dos instrumentos, utilizando o "*alfa* de *Cronbach"* (Hill & Hill, 2002, p.149) e histogramas para comparação de frequências.

2. Validação do questionário e confiabilidade (valor do questionário)

Este questionário foi validado por método "*listwise"* (Maroco, 2003), conforme se apresenta no Quadro 3. Quanto à confiabilidade dos resultados, o valor obtido para o "*alfa* de *Cronbach"*[6] foi 0,626 (Quadro 4). Como se procuram recolher perceções dos grupos da amostra e definir tendências relativamente às quatro variáveis, considera-se que, sob o ponto de vista qualitativo, o valor obtido é aceitável.

Quadro 3 – Resumo do processamento de casos (método *listwise*)

		N	%
Casos	Válido	33	100,0
	Excluídos	0	,0
	Total	33	100,0

Quadro 4 – Estatística de confiabilidade

Alfa de Cronbach	Alfa de Cronbach com base em itens padronizados	N de itens
,626	,629	4

3. Descrição das Variáveis

Foram identificadas quatro variáveis e realizado o seu tratamento estatístico, conforme se apresenta no Quadro 5.

Quadro 5 – Estatística descritiva das variáveis

		VAR01	VAR02	VAR03	VAR04
N	Válido	33	33	33	33
	Omisso	0	0	0	0
Média		2,0909	4,4545	2,0000	4,8182
Mediana		2,0000	4,0000	3,0000	5,0000
Moda		3,00	6,00	3,00	5,00

Legenda:

VAR01 – Maturidade doutrinária (situação atual);

VAR02 – Maturidade doutrinária (situação desejável/futura)

VAR03 – Integração de capacidades operacionais (situação atual)

VAR04 – Integração de capacidades operacionais (situação desejável/futura)

4. Correlação entre Variáveis

Foi analisada a correlação entre as variáveis, nomeadamente, quanto ao seu distanciamento/proximidade utilizando para esse efeito a análise da correlação de *Pearson* (Quadro 6). Os resultados obtidos apontam para a existência das seguintes relações de proximidade: VAR01-VAR03 e VAR02-VAR04. Esta situação, reflete a existência de um nível de maturidade atual (baixo) e futuro (mais elevado) semelhante para estas variáveis. Regista-se uma relação de distanciamento entre: VAR01-VAR02 e VAR03-VAR04.

Quadro 6 –Análise da correlação das variáveis

		VAR00001	VAR00002	VAR00003	VAR00004
VAR00001	Correlação de Pearson	1	,250	,464**	,084
	Sig. (bilateral)		,160	,006	,641
	N	33	33	33	33
VAR00002	Correlação de Pearson	,250	1	,187	,539**
	Sig. (bilateral)	,160		,297	,001
	N	33	33	33	33
VAR00003	Correlação de Pearson	,464**	,187	1	,261
	Sig. (bilateral)	,006	,297		,142
	N	33	33	33	33
VAR00004	Correlação de Pearson	,084	,539**	,261	1
	Sig. (bilateral)	,641	,001	,142	
	N	33	33	33	33

**. A correlação é significativa no nível 0,01 (bilateral).

Conclui-se assim que o relacionamento entre a situação atual e futura é muito reduzido o que prova uma clara perceção da amostra em termos da necessidade de mudança.

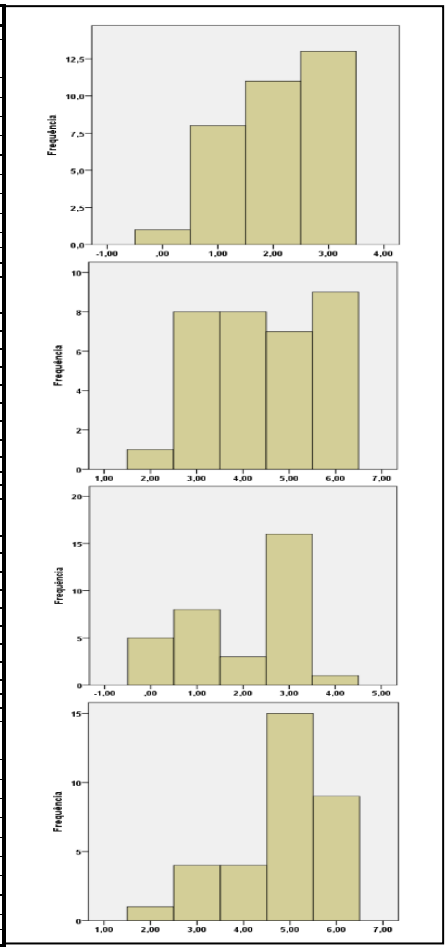
5. Histograma (Frequência)

De forma a melhor analisar a variação das respostas às diversas variáveis, dentro de cada grupo e entre grupos, apresenta-se o seu histograma e os respetivos gráficos de frequência (Quadro 7).

[6] Conforme Hill e Hill (2002, p. 149) o coeficiente "*alfa* de *Cronbach*" é considerado: inaceitável, se ≤0.6; fraco, se [0.6, 0.7[; razoável, se [0.7, 0.8[; bom, se [0.8, 0.9[; e excelente, se ≥0.9.

Quadro 7 –Histograma descritivo e gráficos de frequência das variáveis

			Estatística	Erro Padrão
VAR00001	Média		2,0968	,16300
	95% Intervalo de Confiança para Média	Limite inferior	1,7639	
		Limite superior	2,4297	
	5% da média aparada		2,1434	
	Mediana		2,0000	
	Variância		,824	
	Desvio Padrão		,90755	
	Mínimo		,00	
	Máximo		3,00	
	Amplitude		3,00	
	Amplitude interquartil		2,00	
	Assimetria		-,486	,421
	Curtose		-,951	,821
VAR00002	Média		4,4516	,22642
	95% Intervalo de Confiança para Média	Limite inferior	3,9892	
		Limite superior	4,9140	
	5% da média aparada		4,4821	
	Mediana		4,0000	
	Variância		1,589	
	Desvio Padrão		1,26065	
	Mínimo		2,00	
	Máximo		6,00	
	Amplitude		4,00	
	Amplitude interquartil		3,00	
	Assimetria		-,097	,421
	Curtose		-1,322	,821
VAR00003	Média		1,9677	,22473
	95% Intervalo de Confiança para Média	Limite inferior	1,5088	
		Limite superior	2,4267	
	5% da média aparada		1,9839	
	Mediana		3,0000	
	Variância		1,566	
	Desvio Padrão		1,25124	
	Mínimo		,00	
	Máximo		4,00	
	Amplitude		4,00	
	Amplitude interquartil		2,00	
	Assimetria		-,372	,421
	Curtose		-1,397	,821
VAR00004	Média		4,7742	,19515
	95% Intervalo de Confiança para Média	Limite inferior	4,3756	
		Limite superior	5,1728	
	5% da média aparada		4,8405	
	Mediana		5,0000	
	Variância		1,181	
	Desvio Padrão		1,08657	
	Mínimo		2,00	
	Máximo		6,00	
	Amplitude		4,00	
	Amplitude interquartil		2,00	
	Assimetria		-,851	,421
	Curtose		,134	,821



Em seguida, analisa-se a dispersão das respostas dentro de cada grupo e entre grupos, evidenciando também as diferenças entre a "situação atual" e "situação desejável/futura" para cada uma das variáveis em análise (Figura 18). No caso do grupo mais numeroso (U - utilizadores dos sistemas), para as situações analisadas, a dispersão das respostas é maior, evidenciando uma menor homogeneidade na perceção da realidade. Por esta ordem, o grupo dos Diretores Funcionais (DF), Grupo dos 4 (G4) e grupo dos Comandos Operacionais (CO), apresenta uma visão agregada mais próxima, nas duas situações.

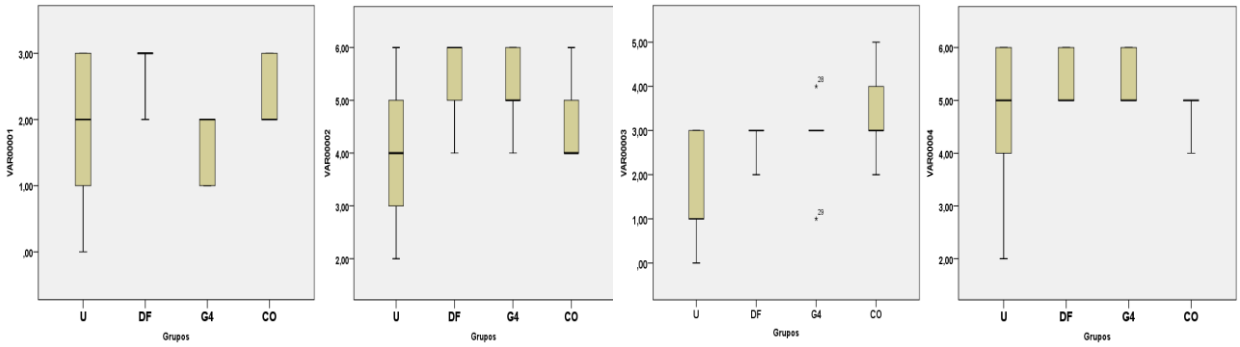


Figura 18 – Dispersão das respostas para todas as variáveis e grupos da amostra

6. Síntese conclusiva

Da análise realizada, conclui-se que:

- A correlação entre a situação "atual" e "futura" é muito reduzida, o que prova uma clara perceção da amostra em termos da necessidade de mudança.
- A relação entre as variáveis caraterizadoras da situação "atual" e "futura" é significativa. Tal reflete a existência de um nível de maturidade atual (baixo) e futuro (mais elevado) semelhante nas duas variáveis.
- A dispersão das respostas dentro de cada grupo é mais significativa ao nível tático/técnico (utilizadores dos sistemas) e mais aproximada ao nível operacional (Diretores Funcionais CSI). A convergência entre grupos é mais evidente e mais positiva no caso da variável "integração de capacidades", a promover.

Apêndice D — Entrevistas a entidades nacionais

Foram realizadas entrevistas presenciais, por correio eletrónico e mistas (entrevista presencial seguidas de respostas escritas) a entidades nacionais ligadas à cibersegurança e ciberdefesa do Estado. A ordem com que são listadas e apresentadas reflete a data de realização/receção da entrevista. Segue-se: resumo do texto e questionário enviado, lista dos entrevistados e os principais resultados obtidos, acrescentando-se, quando possível, a confirmação das dimensões/variáveis e indicadores do modelo de análise.
Nota: as transcrições completas das respostas às questões encontram-se nos arquivos do autor do presente TII.

Texto do guião da entrevista:

Excelentíssimo Senhor,

Chamo-me Paulo Viegas Nunes, Coronel do Exército, e encontro-me a frequentar o Curso de Promoção a Oficial General (CPOG) 2019-2020 no Instituto Universitário Militar (IUM), em Pedrouços.

Integrado no plano de curso, os auditores desenvolvem temas de investigação onde abordam questões relevantes para o futuro das Forças Armadas (FFAA) Portuguesas. Neste contexto, estou a investigar o seguinte tema: "A edificação da capacidade de ciberdefesa nacional".

Sendo Vossa Excelência um reconhecido especialista na matéria que se pretende desenvolver, nomeadamente, no que se refere à caracterização do quadro onde decorre a possível intervenção das várias Entidades nacionais na área da segurança e defesa do ciberespaço, vinha desta forma solicitar a sua resposta sucinta a oito questões que a seguir se apresentam. Se para além das questões apresentadas entender propor outras áreas e linhas de investigação que considere relevantes, ficaríamos profundamente agradecidos.

1. Face ao impacto estratégico do ciberespaço no ambiente de segurança internacional e à necessidade das FFAA defenderem as suas redes e realizarem operações militares neste domínio, importa definir uma estratégia militar para o ciberespaço. Qual considera ser:
   a) O seu âmbito?

   b) A finalidade a atingir?

2. Tendo a *North Atlantic Treaty Organization* (NATO) assumido o ciberespaço como o seu quarto domínio das operações na cimeira de Varsóvia (julho 2016), qual considera ser o impacto desta decisão na condução de operações das FFAA, tanto em tempo de Paz/normalidade como numa situação de crise/conflito?

3. De acordo com a alteração doutrinária operada pela NATO em 2016, qual considera ser o nível de maturidade doutrinária existente e qual deveria ser, em seu entender, a situação a promover no futuro? Por favor, utilize a seguinte tabela na sua resposta, assinalando <u>apenas a opção que considera mais ajustada</u> na situação atual/real e na situação futura/desejável.

Maturidade Doutrinária			
Natureza	**Descrição**	**Situação atual/ real**	**Situação futura/desejável**
Inexistente	Segurança SIC – sem reconhecimento do ciberespaço e do ambiente da informação		
Visão Técnica	Segurança da informação (INFOSEC), atendendo aos desafios técnicos do ciberespaço		
Visão Tática	Segurança da informação e operações defensivas em redes de computadores (INFOSEC+CNO defensivas)		
Visão Operacional	Distribuída (EMGFA + Ramos – Centro de Ciberdefesa)		
	Centralizada (EMGFA – Centro de Operações)		
Visão Estratégica	Militar conjunta (Comando Componente – novo Ramo)		
	Autónoma nacional (Centro de Cibersegurança e Ciberdefesa Nacional)		

4. Face aos constrangimentos existentes, nomeadamente, ao nível dos recursos humanos das FFAA, atendendo aos diferentes modelos orgânicos existentes noutros Países e Organizações Internacionais de que Portugal faz parte (NATO e União Europeia), qual considera ser a estrutura a adotar pelas FFAA no levantamento da sua capacidade de ciberdefesa?

5. Relativamente ao nível da organização em que tem lugar a integração das capacidades existentes, qual considera ser a situação atual e a promover no futuro? Por favor, utilize a seguinte tabela na sua resposta, assinalando apenas a opção que considera mais correta na situação atual/real e na situação futura/desejável.

6.

Integração de Capacidades Operacionais			
Natureza	**Descrição**	**Situação atual/ real**	**Situação futura/desejável**
Não Coordenada	Nível de coordenação residual/inexistente		
Coordenada	Nível de cada Ramo		
	Nível conjunto		
Centralizada	Com coordenação distribuída (EMGFA+Ramos)		
	Com coordenação centralizada (EMGFA)		
Integrada	Nível conjunto (Comando Conjunto - EMGFA+Ramos)		
	Autónoma (novo Ramo e de natureza conjunta)		

6. Tendo por base o processo de desenvolvimento de capacidades militares (estratégia genética), qual considera ser o modelo de desenvolvimento da capacidade de ciberdefesa a adotar pelas FFAA?

7. Atendendo ao facto de a cibersegurança e a ciberdefesa do País exigirem uma estreita cooperação entre todas as Entidades envolvidas, como considera que estas Entidades podem contribuir para dinamizar a edificação da capacidade de ciberdefesa nacional, no plano:
   a) Das sinergias nacionais (*e.g.*, Centro Nacional de Cibersegurança, Centro de Ciberdefesa das FFAA, Polícia Judiciária e Serviços de Informações e Segurança)?
   b) Da cooperação internacional (*e.g.*, NATO e União Europeia)?

8. Deseja apresentar algum comentário ou sugestão?

Muito obrigado por ter respondido às questões formuladas.

#	Entidades	Função
N1	Engenheiro Lino Santos	Coordenador do Centro Nacional de Cibersegurança
N2	Comandante-de- Mar e Guerra Hélder Fialho de Jesus	Chefe do CCD das FFAA
N3	Inspetor-Chefe Carlos Cabreiro	Coordenador da UNC3T
N4	Inspetor-Chefe Rogério Bravo	UNC3T
N5	Representante SIS	Serviços de Informações e Segurança
N6	Brigadeiro-General João Rocha	Diretor CSI /EMGFA
N7	Comodoro Bento Domingues	Superintendente SSI / Marinha
N8	Brigadeiro-General Bento Soares	Diretor CSI /Exército
N9	Major-General Passos Morgado (Reserva)	Diretor CSI /Força Aérea (2017-2020)
N10	Vice-Almirante Silvestre Correia	Comandante Naval
N11	Major-General Xavier de Sousa	2º Comandante das Forças Terrestres
N12	Major-General Maia Pereira	Chefe da Divisão de Planeamento Estratégico Militar do EMGFA (2018-2020) e atual Diretor Coordenador do EME

Principais resultados obtidos de acordo com o modelo de análise:

Conceitos/ Constructos	Dimensões/ Variáveis	Ideias-chave	Indicadores
Estratégia militar para o ciberespaço	Âmbito	O âmbito da EMCIBER é a "proteção das infraestruturas da Defesa e a **condução de operações no/e através do ciberespaço em apoio do Sistema de Forças, incluindo as Forças e Elementos Nacionais Destacados, nos vários domínios de emprego operacional (terra, mar, ar e ciberespaço)**" (N2, N10-N12); "desenvolver a CCDN, articulada com a ENSC, e contribuir para a segurança do ciberespaço de interesse nacional" (N8, N9, N10, N11). "O foco não deve ser a ENCD mas a resiliência das FFAA" (N12).	**Domínio de aplicação** Condução de operações no/e através do ciberespaço em apoio do Sistema de Forças, incluindo as Forças e Elementos Nacionais Destacados, nos vários domínios de emprego operacional (terra, mar, ar e ciberespaço).
	Finalidade	A finalidade a atingir é: a "**garantia da informação**" (N2-N4, N11, N12); "perspetivar a superioridade da informação"(N3-N5); "assegurar a Defesa Nacional no ciberespaço e a liberdade de ação das FFAA" (N1, N6,N7); "**proteção, em permanência, das infraestruturas da Defesa**; **produção de efeitos no e através do ciberespaço; proteção do ciberespaço de interesse nacional**" (N8-N11); "proteção e defesa das infraestruturas críticas nacionais e do governo eletrónico" (N2, N11).	**Nível de ambição:** Garantia da informação e perspetivar a superioridade da informação. **Objetivo a atingir** Proteção, em permanência, das infraestruturas da Defesa; produção de efeitos no e através do ciberespaço; proteção do interesse nacional.
Estratégia operacional para o ciberespaço	Maturidade doutrinária	Alinhamento ao nível G4 (N1-N5), DF (N6-N9) e CO (N10-N12) relativamente ao nível da maturidade doutrinária: **Situação atual**: **Visão técnica/tática** (INFOSEC+CNO defensivas) (G4) (CO); **Visão operacional distribuída** (EMGFA + Ramos – Centro de Ciberdefesa) (DF); **Situação futura**: **Visão estratégica autónoma nacional** (Centro Cibersegurança e Ciberdefesa Nacional integrados) (N2, N4, N7-N9); **Visão Estratégica Militar Conjunta** (Comando Componente –novo Ramo) (N1, N5, N10); **Visão operacional centralizada** (EMGFA–Centro Operações) (N3, N6, N11, N12).	**Nível de maturidade doutrinária**: Situação atual (média): Visão técnica/tática (INFOSEC+CNO defensivas). Situação futura (média): Visão estratégica militar conjunta (Comando Componente –novo Ramo).
	Conceito de operações	O reconhecimento do Ciberespaço como 4.º domínio operacional pela NATO tem o seguinte impacto nas FFAA: "**adoção do ciberespaço como um domínio para a condução de operações, à semelhança do ar, terra e mar (sendo o 4.º domínio)**" (N2-N5, N6, N7); "nestes domínios temos os **três níveis de planeamento: tático, operacional e estratégico. Coordenação centralizada e execução descentralizada, segundo uma lógica multi-domínio**" (N2, N10, N12); "esta decisão tem um **impacto *essencial* e *estruturante*, já que o domínio do espaço cibernético é fundamental para a realização de qualquer tipo de operação militar, independentemente da conjuntura e/ou situação**" (N1, N5, N6, N10); "prioridade ao desenvolvimento da capacidade de ciberdefesa a par dos Países aliados, sendo o **ciberespaço utilizado desde o tempo de Paz/normalidade até uma situação de conflito/crise**" (N1, N3, N7, N8, N10-12); "Prosseguir **desenvolvimento das capacidades de segurança de sistemas e da informação militar e de defesa** e **criar, separadamente uma capacidade autónoma de condução de operações ofensivas no ciberespaço**" (N1). "**Impõe-se uma alteração da cultura e do paradigma operacional**" (N11, N12).	**Conceito de emprego de forças:** Ciberespaço é fundamental para a realização de qualquer tipo de operação militar, independentemente da conjuntura e/ou situação, desde o tempo de Paz/normalidade até situação de crise/conflito". **Conceito de operações:** Adoção do ciberespaço como um domínio para a condução de operações, envolvendo três níveis de planeamento: tático, operacional e estratégico. Coordenação centralizada e execução descentralizada, segundo uma lógica multi-domínio. Segurança dos SIC das FFAA e da Defesa e capacidade autónoma de condução de operações defensivas e ofensivas no ciberespaço.
Estratégia estrutural para o ciberespaço	Estrutura organizacional	Face aos constrangimentos identificados, essencialmente ao nível dos RH, a estrutura organizacional a adotar pelas FFAA deverá ser a seguinte: "**Estrutura mista entre militares e civis**" (N1, N6); "**capacidade deve ser erigida de forma centralizada no EMGFA**, consolidando assim a CCDN" (N3, N8, N10, N11); "**Existência de um comando irá dar corpo a esta realidade, seguindo as boas práticas internacionais, a dependência de uma entidade técnica (DIRCSI) limita âmbito de atuação e a condução de operações, no e a partir do ciberespaço**", **"estrutura conjunta, autónoma e na dependência direta do CEMGFA**" (N2, N3, N8, N9, N10); "**atuação das FFAA deve ser articulada de forma colaborativa com os restantes elementos com responsabilidades no ciberespaço, concretamente o CNCS, a UNC3T e o SIS**" (N1-N5, N11); "**modelo deve ser síncrono com o de países da nossa dimensão**" (N12). "Adotar um modelo capaz de **assegurar no médio prazo (3 a 5 anos) uma capacidade autónoma de formação das FFAA**, formando civis para captação de talentos. Protocolos com indústria e meio académico para ações de formação pontuais/específicas" (N7, N9, N10); "equacionar a **criação de um quadro/estatuto especial para o pessoal que integre a ciberdefesa, de forma a acautelar a progressão de carreiras e, consequentemente, o recrutamento e a retenção de pessoal**" (N1, N7, N10); "**o objetivo da edificação da capacidade não vai ser atingido sem RH qualificados, comprometendo a capacidade para conduzir operações no ciberespaço**" (N9, N11, N12).	**Modelo organizacional:** A estrutura a adotar deve conjunta, autónoma e na dependência direta do CEMGFA, assumindo a forma de um comando operacional. Estrutura mista incluindo militares e civis. Dependência de uma entidade técnica (DIRCSI) limita âmbito de atuação e a condução de operações, no e a partir do ciberespaço. Em linha com a ENSC, a atuação das FFAA deve ser articulada de forma colaborativa com os restantes elementos com responsabilidades no ciberespaço (CNCS, a UNC3T e o SIS). **Quadros orgânicos**: Equacionar criação de quadro especial para pessoal que integre a ciberdefesa, de forma a acautelar progressão de carreiras, o recrutamento e a retenção de pessoal. Assegurar formação e qualificação do pessoal afeto à área da ciberdefesa. Objetivo da edificação da capacidade não será atingido sem pessoal qualificado; afeta capacidade condução operações no ciberespaço.

Conceitos/ Constructos	Dimensões/ Variáveis	Ideias-chave	Indicadores
Estratégia estrutural para o ciberespaço	Integração de capacidades operacionais	Relativamente à integração de capacidades operacionais verifica-se que existe um alinhamento ao nível G4 (N1-N5) e DCSI (N6-N9): **Situação atual**: **Centralizada com coordenação distribuída** (EMGFA+Ramos) (N1, N2, N5-N9, N10); coordenada ao nível de cada Ramo (N4, N11) ou ao nível conjunto (N12) **Situação futura**: **Integrada ao nível conjunto (comando conjunto - EMGFA+Ramos).** (N1, N3-N8, N11); Integrada e autónoma (novo Ramo e de natureza conjunta) (N2, N9, N10 e N7 – dupla escolha).	**Nível da integração de capacidades operacionais:** Situação atual (média): **Centralizada com coordenação distribuída** (EMGFA+Ramos). Situação futura (média): **Integrada ao nível conjunto** (Comando Conjunto - EMGFA+Ramos) ou **integrada e autónoma** (novo Ramo e de natureza conjunta).
Estratégia genética para o ciberespaço	Processo de desenvolvimento da capacidade	Relativamente ao processo de desenvolvimento de capacidades: "Devem ser salvaguardados dois pilares fundamentais: **Visão** (que deve ser objetiva, abrangente e pragmática) e **Missão** (que deve garantir a utilização do espaço Ciber)" (N9); "Já existe um **modelo de desenvolvimento dos vetores de capacidade assente no DOTMLPII da NATO e o plano de implementação está aprovado pelo CEMGFA". "Deve ser integrado no CPDM**" (N6-N9, N10- N12);"Modelo deverá ter: **Doutrina** nacional para a ciberdefesa (adaptada da doutrina aliada) (N11, N12); **Organização** com forte componente técnica/científica, um estado-maior; um centro de operações de ciberdefesa (N2, N11); **Liderança** ao nível OF6/OF7 (N2); **Equipamento e ferramentas** HW e SW "*state of art*" (N2, N11); "**Recursos Humanos** com elevado nível de formação, vocação e inamovíveis por períodos mínimos de 5 anos; (N1-N5); Quadro especial (N11, N12); "**Infraestruturas** adequadas à dimensão do órgão, dotadas de elevados níveis de segurança física e eletrónica" (N2, N11, N12); **Interoperabilidade** total com o CNCS e atores externos civis e militares." (N8, N11); "Recurso a modelo centralizado, que depende da decisão política" (N3). "**Capacidade de recrutar de forma complementar aos Ramos**. Sendo esta uma área nova e onde existem poucos RH, tem de existir uma **valorização dos militares e civis afetos à ciberdefesa**". (N2, N9, N12)	**Plano de implementação da capacidade:** Modelo de desenvolvimento de capacidades DOTMLPII, de acordo com o plano de implementação aprovado pelo CMGFA e integrado com o CPDM. Neste processo deve ser sempre salvaguardada a visão estratégica formulada, e a missão a cumprir (garantir utilização espaço Cyber). **Vetores de desenvolvimento da Capacidade:** **Doutrina** nacional para a ciberdefesa (adaptada da doutrina aliada); **Organização** com forte componente técnica/científica, um Estado-Maior; um Centro de Operações de Ciberdefesa; **Liderança** ao nível OF6/OF7; **Equipamento** e ferramentas HW e SW "*state of art*"; **Pessoal** com elevado nível de formação, vocação e inamovíveis por períodos mínimos de 5 anos; quadro especial; **Infraestruturas** adequadas à dimensão do órgão, dotadas de elevados níveis de segurança física e eletrónica; **Interoperabilidade** total com o CNCS e atores externos civis e militares.
	Sinergias nacionais	As sinergias nacionais (*e. g*., CNCS, CCD, PJ e SIS) podem contribuir para dinamizar a edificação da capacidade de ciberdefesa através de: "**protocolos de colaboração e de partilha de informação interagência**" (N1, N10, N3-N5, N7, N8, N11); "**Cooperação deve passar pela integração de RH em equipas multidisciplinares e intersectoriais (oficiais de ligação)**, podendo, ainda, estender-se à participação /integração de elementos, fora do âmbito da Defesa, em exercícios onde participam as FFAA" (N1-N5, N10, N11); "podem ser consideradas formações combinadas, agregando setores/grupos heterogéneos" (N2, N3, N10, N11); "**a criação de plataformas comuns de partilha de informação, permite também assegurar a interoperabilidade**, potenciando, assim, respostas em tempo e consequentemente uma melhor segurança do ciberespaço" (N1-N3, N5, N6, N8, N10). Nos 8 vetores de desenvolvimento da capacidade, os aspetos mais importantes são o "Treino, Material e interoperabilidade (agrega os dois anteriores)" (N2, N10, N11).	**Organizações nacionais:** Protocolos de cooperação e adoção de modelo de cooperação operacional interagência - C4 (CNCS, CCD, UNC3T e SIS). Explorar a possibilidade da integração de quadros em equipas multidisciplinares (oficiais de ligação) ao nível de atividades operacionais e exercícios. **Projetos de ID&I:** Potenciar a interoperabilidade, adotando plataformas comuns sempre que ajustado como a plataforma de partilha de informação entre o C4 (Projeto NATO MISP). Potencia rapidez na resposta e reforça a cibersegurança nacional.
	Cooperação internacional	A cooperação internacional (*e. g*., NATO e UE) podem contribuir para dinamizar a edificação da capacidade de ciberdefesa através de: "presença em fóruns, organizações e participação em exercícios é fundamental para a dinamização e alinhamento da capacidade" (N2, N6, N10, N11); **Garantir a presença nacional** no NCIRC, CCDCOE, *NCI Academy*, em **exercícios** como o *Cyber Coalition*, *CWIX* ou *Locked Shields* e em **fóruns** como o *Cyber Defence Research & Technology* da EDA - permitem **melhorar procedimentos, garantir interoperabilidade** e criar **melhor conhecimento na segurança do ciberespaço**" (N2, N10, N11). "A **utilização de plataformas comuns de trabalho e de partilha de informação**, beneficia a interoperabilidade e a reação em uníssono a eventos" (N2, N6, N10, N11). "**Potencia o desenvolvimento de Doutrina, da Organização, do Treino e da Liderança**" (N10, N11). Portugal tem vindo a afirmar-se nas áreas: E&T- liderança do Projeto NATO de Smart Defence MNCDE&T; liderança da *Cyber Defence Discipline* da UE; da adesão ao CCD CoE; Exercícios: liderança da *focus area* de ciberdefesa (desde 2018) no exercício CWIX da NATO; no fórum ibero-americano de ciberdefesa, onde propôs a adoção de uma plataforma de partilha de informação para esta comunidade (em concretização) (N1, N6, N7).	**Organizações internacionais:** Cooperação internacional pode contribuir para reforçar o desenvolvimento de capacidades, nomeadamente ao nível NATO e da EU. **Projetos internacionais:** Portugal tem tido reconhecimento internacional significativo nas áreas: educação e treino, através da liderança do Projeto NATO de Smart Defence MNCDE&T, da liderança da *Cyber Defence Discipline* da UE; da adesão ao CCDCOE, na liderança da *focus area* de ciberdefesa (desde 2018) no exercício CWIX (o maior exercício de interoperabilidade da NATO); no fórum ibero-americano de ciberdefesa, onde propôs a adoção de uma plataforma de partilha de informação para esta comunidade (em concretização).

Apêndice E — Linhas orientadoras, requisitos e alinhamento estratégico da EMCIBER

Valores	Nível de Ambição	Linhas Orientadoras (LO)	Requisitos Estratégicos (RE)	Objetivos a atingir – Requisitos Operacionais (RO) (aspetos a considerar pela EMCIBER)	Alinhamento	
					DEEMGFA 2018-2021	ENSC 2019-2023 (Eixos)
Proteção e Sustentação **Proporcionalidade e Credibilidade** **Parceria e Cooperação**	**Assegurar em permanência a proteção das infraestruturas de Defesa, a condução de operações no ciberespaço em apoio ao Sistema de Forças, incluindo as Forças e Elementos Nacionais Destacados e contribuir proactivamente para a segurança do ciberespaço de interesse nacional e a projeção internacional de Portugal**	**LO1 - Prosseguir o desenvolvimento da capacidade de ciberdefesa nacional**, tendo em vista maximizar a resiliência das FFAA para fazer face a incidentes ou ciberataques significativos que afetem os interesses e a soberania nacionais.	**RE1 - Reforçar a capacidade de ciberdefesa nacional**, garantindo a proteção, a resiliência e a segurança das redes e dos SIC da Defesa contra ciberataques.	**RO1 -** Reforçar o efetivo dos RH afetos às estruturas de ciberdefesa. **RO2** – Modernizar e sustentar a atualização periódica do parque informático e das soluções de rede da Defesa Nacional, de forma a aumentar a resiliência das FFAA face a ciberataques. **RO3** – Garantir a evolução futura das plataformas e ferramentas de segurança de forma a reforçar a defesa dos sistemas de C2, dos sistemas de armas e das infraestruturas da Defesa. **RO4** – Consolidar as condições das infraestruturas afetas à ciberdefesa nacional, tendo em vista as necessidades futuras.	Melhorar capacidade ciberdefesa nacional (LA2.02)	Estrutura de segurança do ciberespaço (Eixo 1) Proteção do ciberespaço (Eixo 3)
		LO2 - Reforçar o potencial militar de conduzir operações no ciberespaço, assegurando a liberdade de ação do país no ciberespaço, em salvaguarda da defesa do interesse nacional e da afirmação da soberania nacional neste domínio.	**RE2 - Desenvolver a capacidade militar de conduzir operações no ciberespaço,** a fim de salvaguardar a defesa do interesse nacional, a afirmação da soberania nacional neste domínio e contribuir para a dissuasão.	**RO5** – Adequar a estrutura da ciberdefesa nacional de forma a reforçar a capacidade para conduzir OpCiber. **RO6 -** Levantar uma capacidade eficiente e eficaz de CNO (defensivas, exploração e ofensivas), garantindo a liberdade de ação do País e negar o seu uso hostil contra o interesse nacional. **RO7** – Assegurar treino coletivo e individual de forma a atingir níveis de atuação ajustados à gestão de crises. **RO8** – Incrementar o nível de sensibilização para a ciberdefesa. **RO9** – Satisfazer a resposta estrutural e operacional da ciberdefesa face aos desafios futuros, adotando uma abordagem integrada, abrangente e articulada às ameaças e riscos do ciberespaço.	Melhorar capacidade ciberdefesa nacional (LA2.02) Incrementar sensibilização ciberdefesa (LA2.04)	Resposta às ameaças (Eixo 4)
		LO3 - Incrementar a cooperação nacional e internacional, tendo em vista a colaboração para garantir a segurança do ciberespaço.	**RE4 - Intensificar a cooperação nacional e internacional,** afirmando Portugal como coprodutor de segurança internacional, contribuindo de forma cooperativa e sinérgica para a segurança do ciberespaço.	**R10 -** Incrementar a coordenação e cooperação entre as diversas entidades nacionais e internacionais na segurança do ciberespaço. **R11** – Sendo o vetor militar relevante para apoio à política externa, importa incrementar a participação e integração em exercícios e em organismos internacionais relevantes na segurança do ciberespaço. **R12 -** Potenciar uma maior maturidade da ciberdefesa nacional e contribuir para a segurança dos nossos parceiros estratégicos.	Contribuir para ENCD e Plano de Ação (LA2.01) Reforçar ligações do CCD (LA2.03)	Cooperação nacional e internacional (Eixo 6)
		LO4 – Aprofundar o conhecimento do ciberespaço, promovendo a formação, autonomia tecnológica e a retenção de talentos.	**RE5 - Valorizar o conhecimento do ciberespaço** e das ameaças associadas reforçando o potencial humano.	**RO13 -** Fomentar a formação e o conhecimento específico em ciberdefesa. **RO14 -** Potenciar ligação às estruturas de ensino e formação nacionais e internacionais.	Incrementar envolvimento do IUM (LA2.05)	Prevenção, educação e sensibilização (Eixo 2)
			RE6 - Promover a ID&I no ciberespaço, incentivando o duplo uso, estabelecendo uma posição de conhecimento, de iniciativa no ciberespaço de interesse nacional.	**RO15 -** Fomentar sinergias nacionais e esforços cooperativos em curso nas organizações internacionais de que Portugal faz parte para, em colaboração com as universidades, os institutos e a indústria, desenvolver soluções tecnológicas para duplo uso, civil e militar. **RO16**– Incentivar/reforçar interoperabilidade da ciberdefesa com atores externos.	Incrementar envolvimento do IUM (LA2.05)	ID&I (Eixo 5)

Fonte: MDN (2019b), EMGFA (2019b) e ENSC (2019).

Apêndice F — Operações no ciberespaço – responsabilidades de C2

No âmbito da condução de OpCiber, tendo por base as relações de C2 existentes e a estabelecer no futuro, importa identificar as responsabilidades e a autoridade a exercer pelos órgãos das FFAA, aos diferentes níveis (estratégico, operacional e tático/técnico). Sem prejuízo de um aprofundamento posterior, tendo por base a doutrina NATO (2013; 2019a; 2019b), especialmente o AJP-3.20 (2020), este apêndice reflete a articulação entre as componentes estrutural e operacional da EMCIBER, conforme ilustrado na Figura 19.

1. Nível estratégico

O CEMGFA, como em todas as operações das FFAA, assume o papel de Comandante de nível estratégico das OpCiber e, apoiado pelo Comando Conjunto das FFAA, assume a autoridade da sua coordenação em todos os teatros de operações. O CEMGFA assegura também o comando operacional das FND quando empenhadas em operações ou missões de cariz multinacional. O comandante do COCIBER constitui o principal conselheiro do CEMGFA para este domínio operacional.

O COCIBER assume o papel de Comando de Componente de teatro para o ciberespaço, estabelecendo a fronteira entre o planeamento de efeitos de nível estratégico e operacional. Este Comando, constitui o ponto focal para todas as operações neste domínio, assumindo o papel de autoridade coordenadora da ciberdefesa. O COCIBER assume também o papel de integrador de forças e capacidades militares no ciberespaço, assim como o de autoridade de gestão dos serviços de Comunicações e Sistemas de Informação (CSI) para a rede de operações das FFAA e da Defesa.

2. Nível operacional

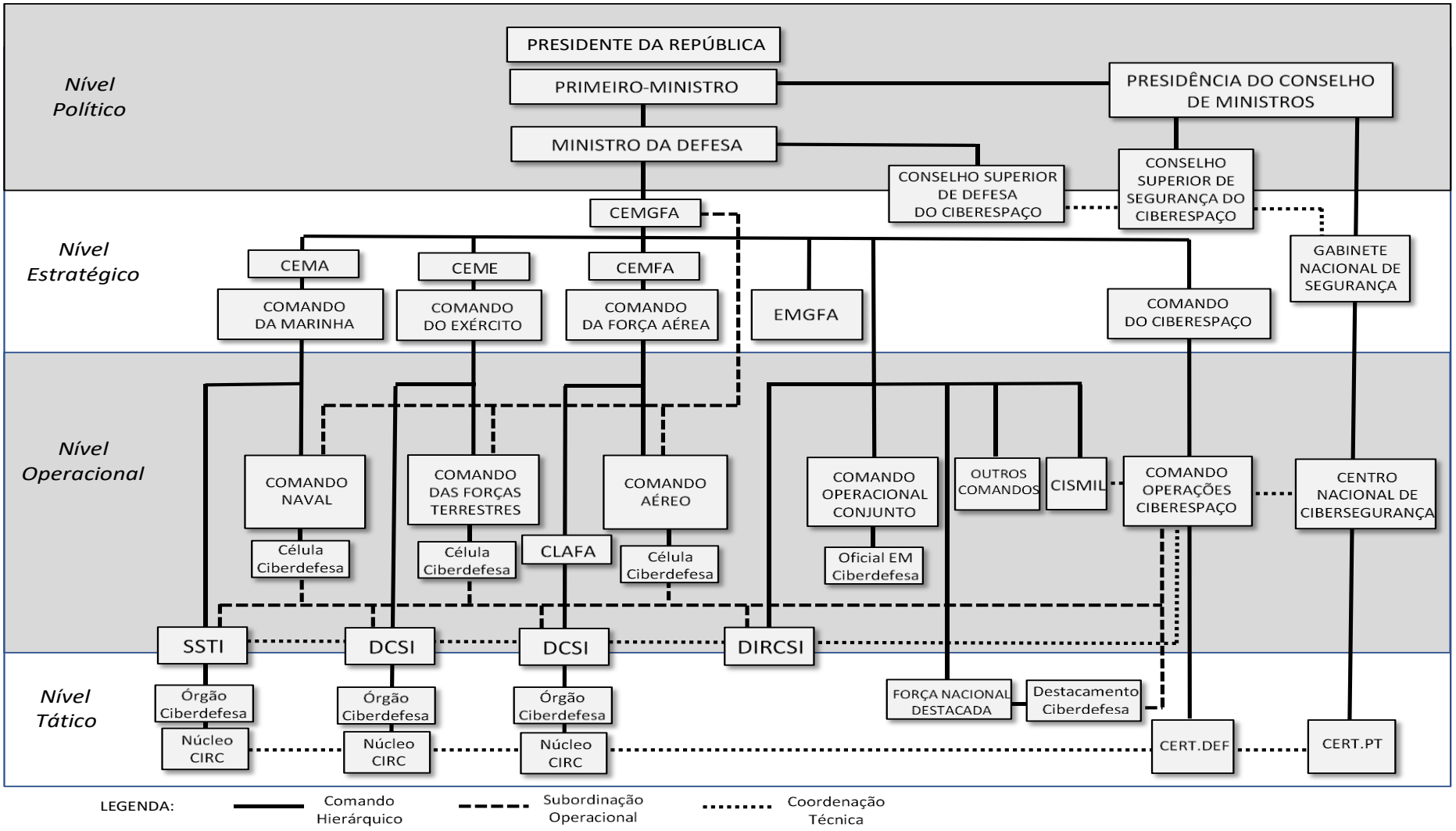
O COCIBER garante a coesão da articulação e atuação operacional das FFAA no ciberespaço. Apoia todos os elementos de nível operacional e tático (CSI do EMGFA e Ramos) no planeamento, preparação e condução de atividades e operações conjuntas. Garantindo o conhecimento situacional no ciberespaço, o COCIBER apoiará e será apoiado por todos os elementos de nível operacional com a troca de informações e relato de eventos no ciberespaço. Neste contexto, assume especial importância a existência de uma ligação permanente e sinérgica com o Centro de Informações e Segurança (CISMIL) das FFAA, permitindo assegurar uma eficaz *Intelligence Surveillance and Reconnaissance* (ISR) no ciberespaço e a manutenção de uma *cyber common operational picture*, consistente e tão precisa quanto possível. O desenvolvimento de sinergias entre as diferentes capacidades (CSI e ISR) e uma cooperação próxima na preparação e execução das missões atribuídas ao COCIBER serão decisivas para o seu sucesso operacional.

Todos os Comandos Operacionais e eventuais Quartéis-Generais dos Comandos de Componente, no cumprimento das suas missões, planeiam, preparam e conduzem atividades e operações na área/domínio que lhes for atribuído, tendo em conta os aspetos ligados à sua proteção no ciberespaço e resiliência operacional. Desta forma, para além das estruturas CSI necessárias ao seu C2, estes Comandos deverão integrar uma célula de ciberdefesa na sua orgânica. Para além de operações de proteção CSI e defensivas, estas células podem receber autoridade delegada do COCIBER para a condução de outras atividades operacionais no ciberespaço, assumindo para esse efeito o papel de gestor de serviços de segurança CSI na sua área de operações. Em particular, quando se trate de uma FND, no âmbito de uma operação multinacional ou fora de área, a ciberdefesa da Força poderá ser assegurada por um destacamento de ciberdefesa.

Em caso de empenhamento operacional do COCIBER numa operação conjunta, este Comando assume a coordenação operacional de todos os SIC e órgãos de ciberdefesa das FFAA (nível EMGFA, Ramos e Defesa). No contexto da cibersegurança nacional, assumindo o papel de autoridade nacional para a ciberdefesa, o COCIBER assegura também ao nível operacional uma coordenação permanente com o CNCS, a UNC3T e o SIS.

3. Nível tático/técnico

A DIRCSI do EMGFA, assumindo o papel de autoridade técnica, é responsável pela coordenação técnica dos SIC que apoiam o C2 do EMGFA e das FND. As operações CSI das FFAA (EMGFA e Ramos), para além de integradas ao nível conjunto, devem ser estreitamente coordenadas com o COCIBER, nomeadamente, para assegurar a necessária unidade de comando e esforço no âmbito da realização de OpCiber.



CEMA – Chefe do Estado-Maior da Armada; **CEMFA** – Chefe do Estado-Maior da Força Aérea; **CEMA** – Chefe do Estado-Maior do Exército; **CEMGFA** – Chefe do Estado-Maior-General FFAA; **CERT** – *Computer Emergency Response Team*; **CIRC** – *Computer Incident Response Capability*; **CISMIL** – Centro de Informações Militares; **CLAFA** – Comando Logístico da Força Aérea; **DCSI/DIRCSI** – Direção de Comunicações e Sistemas Informação; **EM** – Estado-Maior; **SSTI** – Superintendência de Sistemas e Tecnologias de Informação.

Figura 19 – Estrutura da ciberdefesa nacional

Todos os Ramos possuem uma Direção CSI, responsável pela gestão integrada das suas redes e pelo planeamento do emprego dos respetivos SIC orgânicos (fixos e projetáveis). Os órgãos responsáveis pela ciberdefesa dos Ramos, onde se inserem os núcleos CIRC, dependem das respetivas Direções CSI. A segurança da informação que circula nas redes das FFAA é coordenada pelo COCIBER que, através do seu CERT.DEF e dos CIRC dos Ramos, assegura a resposta a incidentes de segurança. Para esse efeito, integrando a rede nacional de CSIRT, o CERT.DEF mantém também uma ligação permanente ao CERT.PT e ao NCIRC, garantindo assim uma resposta sinérgica e cooperativa tanto no plano nacional como internacional.

4. Execução – visão geral

Constituindo a Aliança Atlântica a fonte doutrinaria das FFAA portuguesas, no que se refere às operações CSI e às operações defensivas no ciberespaço, importa reconhecer que os seus fundamentos (NATO, 2016b), se encontram intimamente ligados ao planeamento, desenvolvimento e gestão de redes operacionais e serviços C2, definidos no quadro da implementação do conceito de *Federated Mission Networking*, em curso tanto no contexto NATO como nacional. Relativamente à condução de operações ofensivas no ciberespaço, a NATO é relativamente omissa porque, assumindo uma postura defensiva e atendendo aos constrangimentos políticos e operacionais das OpCiber, considera apenas a possibilidade de integrar na sua resposta operacional os efeitos produzidos por nações aliadas, a título nacional e voluntário, os designados *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA).

A condução de operações ofensivas constitui assim uma capacidade soberana e inalienável de cada nação aliada. Isto significa que, para garantir às FFAA uma capacidade acrescida para defender as suas redes contra ciberataques e realizar operações militares no ciberespaço, o COCIBER terá que dispor de uma capacidade CNO credível, dissuasora e eficaz. Quando aplicável, num cenário de defesa coletiva, as capacidades nacionais podem ser reforçadas pelos efeitos SCEPVA. Neste caso, estas operações serão coordenadas e conduzidas como parte do ciclo de *targeting* conjunto da Aliança, obedecendo aos procedimentos e requisitos existentes para esse efeito. De forma similar, para a gestão da recolha de informação ISR, as OpCiber utilizarão o sistema conjunto ISR e o ciclo de recolha de informação NATO. Conforme se ilustra no Quadro 8, os quatro tipos de atividades operacionais envolvidas nas OpCiber, antes apresentados, são desenvolvidos ao longo das diversas fases do *NATO Crisis Response Process* (NCRP) (NATO, 2019e). Com os necessários ajustamentos, atendendo à natureza do empenhamento das FFAA no ciberespaço, considera-se que estes princípios e processos doutrinários também se aplicam à realidade nacional.

Quadro 8 – Operações a desenvolver na resposta a crises

<table>
<tr><td colspan="7">Federated Mission Networking</td></tr>
<tr><td>Fases do NCRP
Atividade</td><td>Fase 1:
Indicações e alerta</td><td>Fase 2:
Avaliação da situação</td><td>Fase 3:
Desenvolvimento da resposta</td><td>Fase 4:
Planeamento</td><td>Fase 5:
Execução</td><td>Fase 6:
Transição</td></tr>
<tr><td>Operações CSI</td><td colspan="6" rowspan="2">Minimum Level of Command and Control Service Capabilities in Support of Combined Joint NATO Led Operations (NATO, 2016b)</td></tr>
<tr><td rowspan="2">Operações Defensivas</td></tr>
<tr><td colspan="2" rowspan="2"></td><td colspan="4" rowspan="2">Sovereign Cyber Effects Provided Voluntarily by Allies</td></tr>
<tr><td>Operações Ofensivas</td></tr>
<tr><td>Operações ISR no ciberespaço</td><td colspan="6">Joint Intelligence, Surveillance and Reconnaissance</td></tr>
</table>

Fonte: Adaptado de NATO (2019a, p.6).

As relações de C2, na transição para uma situação de crise/conflito, devem ser ajustadas, variando de acordo com as responsabilidades e autoridades associadas a cada entidade/organização do Estado, respeitando o papel que lhes é atribuído pela Constituição da República Portuguesa. Numa situação de normalidade, as FFAA desenvolvem essencialmente operações CSI e defensivas ao nível estratégico, operacional e tático/técnico. As operações de *intelligence*, ISR e outras atividades desenvolvidas no ambiente de informação pelas FFAA, apoiam também estas operações. Numa situação de crise e conflito/guerra estas atividades são ampliadas e reforçadas pelas operações ISR e ofensivas.

O ambiente de segurança atual, exige às FFAA uma capacidade permanente para deter ciberataques de larga escala, garantindo a ciberdefesa do País e o cumprimento da sua missão (*mission assurance*). A sua estrutura de ciberdefesa, envolvendo a capacidade para conduzir de forma eficaz todos os tipos de CNO (defesa, exploração e ataque), deve assim estar preparada para se ajustar e fazer face a uma situação de crise/conflito, com tempos de alerta e transição mínimos.

Apêndice G — Enquadramento jurídico das operações no ciberespaço

1. Enquadramento

A transversalidade das áreas relacionadas com o ciberespaço e a complexidade associada à condução de operações militares neste domínio, faz com que o quadro jurídico-constitucional aplicável seja relativamente extenso, se encontre disperso e que o ordenamento jurídico tenha que se adaptar à contínua evolução da realidade a regular. Reconhecendo as limitações apontadas, analisou-se a situação internacional e nacional referente ao quadro do levantamento da EMCIBER, incluindo a condução de OpCiber e a própria utilização do ambiente da informação pelas FFAA.

2. Considerações legais sobre o uso da força no ciberespaço

Enquanto *global common*, o ciberespaço não apresenta espaços de soberania claramente definidos. Aproveitando as lacunas legais existentes e as dificuldades de regulamentação daí decorrentes, o aumento dos ciberataques, essencialmente os de natureza mais disruptiva e/ou destrutiva, potencia o uso da força e a ocorrência de conflitos armados no ciberespaço. Esta situação, requer um esforço concertado da comunidade internacional, capaz de promover o ajustamento do direito internacional e fazer convergir o quadro legal nacional de forma articulada. Como parte deste esforço, Portugal já incorporou na ordem jurídica interna acordos/diretivas NATO e legislação da UE, conforme se apresenta no Quadro 9.

Quadro 9 – Legislação internacional incorporada na ordem jurídica interna

Tipo de Legislação	Identificação do documento legal
Legislação Internacional - NATO	
Acordo sobre a Segurança da Informação entre os Estados Parte da NATO	Resolução da Assembleia da República n.º 15/2000, de 6 de março. Promulgado pelo Decreto do Presidente da República n.º 3/2000, de 6 de março. Ratifica o acordo concluído a 06 de março de 1997.
C-M (2002)49 - Security within NATO	*Public Disclosure – PDN (2004)0001 dated 10 Sep.2004*
AC-35-D/2000-REV7	*Directive on Personnel Security*.
AC-35-D/2001-REV2	*Directive on Physical Security*.
AC-35-D/2002-REV4	*Directive on the Security of Information.*
AC-35-D/2003-REV5	*Directive on Industrial Security.*
AC-35-D/2004-REV3	*Primary Directive on CIS Security*.
AC-35-D/2005-REV2	*INFOSEC Management Directive for CIS*.
Legislação Internacional - UE	
Proteção das Informações Classificadas Trocadas no Interesse da UE	Resolução da Assembleia da República n.º 125/2012, de 26 de setembro. Promulgado pelo Decreto do Presidente da República n.º 152/2012, de 26 setembro. Ratifica o Acordo entre os Estados membros da UE, reunidos no Conselho, assinado em Bruxelas em 25 de maio de 2011.
Regras de segurança aplicáveis à Proteção das Informações Classificadas da UE	Decisão n.º 2013/488/UE, do Conselho, de 23 de setembro. Decisão (UE/EURATOM) n.º 2015/444, da Comissão, de 13 de março de 2015.
Luta contra as formas graves de Criminalidade	Decisão n.º 2002/187/JAI, do Conselho, de 28 de fevereiro de 2002-criação da Eurojust

Identificando o ciberespaço como área de confrontação estratégica, a NATO (2014a) reconheceu, na Cimeira de Gales, a aplicabilidade do direito internacional no ciberespaço e que "um ciberataque pode constituir um ataque armado suscetível de desencadear a ativação do artigo 5.º do Tratado de Washington, devendo a sua aplicação ser apreciada, caso a caso, pelo NAC" (NATO, 2014b). Os ciberataques conduzidos contra a Aliança, por atores Estado e não-Estado, que se situem abaixo do limiar de um ataque armado, serão enquadrados numa resposta articulada no contexto do artigo 4.º da Aliança.

Devido às suas implicações estratégicas, as OpCiber conduzidas em tempo de Paz e no contexto das missões NATO, terão também que ser aprovadas pelo NAC, nomeadamente, quanto à sua legitimidade. Reconhecendo a aplicação do direito internacional, a NATO defende que os princípios da necessidade militar, humanidade, proporcionalidade e distinção se aplicam às OpCiber (AJP-3.20, 2020, p.22). Neste âmbito, os conflitos entre Estados são regulados pela Carta da Organização das Nações Unidas ([ONU],1945), que legitima no seu artigo 51.º o recurso ao uso da força (*jus ad bellum*), e pela principal fonte de direito humanitário internacional, a Convenção de Genebra ([CG], 1949), que regula a condução dos conflitos armados (*jus in bello*).

Como ação de contornos agressivos, um ciberataque pode traduzir-se numa utilização da força e constituir um ato de violência não cinética e/ou cinética. Para caracterizar uma situação de uso efetivo da força no ciberespaço, o Manual de Tallinn 2.0 (Schmitt, 2017) analisou a aplicação de um leque alargado de princípios e regras do direito internacional. Este manual doutrinário, reconhece que um ataque armado é a forma mais grave de uso da força, mas que nem todo o uso da força constitui um ataque armado. Um ciberataque que cause uma interrupção pontual de serviços não essenciais não pode ser considerado um ataque armado. No entanto, se este tiver um impacto destrutivo e/ou disruptivo de longo prazo, afetando infraestruturas críticas ou serviços essenciais para a sobrevivência de um Estado, tal consubstancia um ataque armado no ciberespaço, aplicando-se a legislação que rege os conflitos armados (*jus in bello*).

3. Enquadramento jurídico nacional das operações no ciberespaço

Numa sociedade em rede, diversas funções e operações das FFAA dependem de recursos privados e sistemas comerciais sobre as quais estas não detêm qualquer controlo direto ou autoridade. De forma a mitigar os riscos associados a esta dependência, as FFAA terão que estabelecer parcerias e desenvolver sinergias com os seus fornecedores de serviços de forma a reforçar a sua postura defensiva no ciberespaço. Para esse efeito, as FFAA devem respeitar a legislação em vigor, tanto em tempo de Paz/normalidade como numa situação de crise ou guerra.

Pela sua importância para o enquadramento jurídico-constitucional da atuação das FFAA no ciberespaço, no âmbito nacional, para além da legislação avulsa existente, salientam-se os diplomas legais apresentados nos Quadros 10 e 11.

Quadro 10 – Legislação associada à área da segurança e defesa do ciberespaço

Tipo de Legislação	Identificação do documento legal
Constituição da República Portuguesa	VII Revisão Constitucional, de Resolução da Assembleia da República n. º15/2005, 07 abril. Revisão da Constituição da República, aprovada pela Assembleia Constituinte, 02 de abril de 1976.
Estratégia Nacional de Segurança do Ciberespaço	Resolução do Conselho de Ministros n.º 92/2019, de 05 de junho. (2019) - Diário da República, 1.ª Série, 108. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.
Conselho Superior de Segurança do Ciberespaço	Resolução do Conselho de Ministros n.º 115/2017, de 13 de julho - Diário da República, 1.ª Série, 163/2017. Cria o grupo de projeto denominado «Conselho Superior de Segurança do Ciberespaço»
Centro Nacional de Cibersegurança.	Decreto-Lei n.º 69/2014, de 09 de maio de 2014. Aprova a criação do CNCS.
Legislação Nacional - área da Defesa	
Conceito Estratégico de Defesa Nacional	Resolução do Conselho de Ministros n.º 19/2013, de 21 de março – Diário da República, n.º 67, 1.ª Série, 05 de abril. Aprova o Conceito Estratégico de Defesa Nacional.
Lei de Defesa Nacional	Lei Orgânica n.º 05/2014, 29 de agosto. 1.ª alteração à Lei, aprovada pela Lei Orgânica n.º 1-A/2009, de 07 de julho.
Lei Orgânica de Bases da Organização das Forças Armadas	Lei Orgânica n.º 06/2014, 01 de setembro. Alteração da Lei, aprovada pela Lei Orgânica n.º 1-A/2009, de 7 de julho.
Lei de Programação Militar	Lei n.º 02/2019, de 17 de junho – Diário da República, n.º 114, 1.ª Série -A, 17 de junho de 2019. Aprova a Lei de programação militar e revoga a Lei Orgânica n.º 7/2015, de 18 de maio.
Reforma da "Defesa 2020"	Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril – Diário da República n.º 77, 1.ª Série, de 19 de abril. Aprova as linhas orientadores para execução da reforma estrutural da Defesa Nacional e das FFAA, Reforma "Defesa 2020".
Missões Internacionais e Cooperação Técnico-Militar	Lei n.º 46/2003, de 22 de agosto – Diário da República, n.º 193, I Série -A, 22 de agosto de 2003. Regula o acompanhamento, pela AR, do envolvimento de contingentes militares portugueses no estrangeiro.
Estatuto dos Militares das Forças Armadas	Decreto-Lei n.º 90/2015, de 29 de maio – Diário da República, n.º 104, 1.ª Série, 29 de maio de 2015. Aprova o Estatuto dos Militares das Forças Armadas.
Serviço Militar	Lei Orgânica n.º 1/2008, de 06 de maio - Diário da República, n.º 87, 1.ª Série, de 06 de maio de 2008.Primeira alteração à Lei do Serviço Militar, aprovada pela Lei n.º 174/99, de 21 de setembro.
Disciplina e Justiça Militar	Lei n.º 100/2003, de 15 de novembro - Diário da República, n.º 265, I Série -A, de 15 de novembro de 2003.Aprova o novo Código de Justiça Militar e revoga a legislação existente sobre a matéria
Mobilização e requisição no interesse da Defesa Nacional	Lei n.º 20/95, de 13 de julho - Diário da República, n.º 160, I Série -A, de 13 de julho de 1995. Regula a mobilização e a requisição no interesse da Defesa Nacional.
Autoridade Nacional de Emergência e Proteção Civil (ANEPC)	Decreto-Lei n.º 45/2019, de 01 de abril - Diário da República. n.º 64, 1.ª Série, de 01 de abril de 2019. Aprova a orgânica da Autoridade Nacional de Emergência e Proteção Civil (ANEPC).
Regime do Estado de Sítio e do Estado de Emergência	Lei Orgânica n.º 1/2012, de 11 de maio - Diário da República, n.º 92, 1.ª Série, de 11 de maio de 2012.
Sistema de Informações da República Portuguesa (SIRP) e Serviço de Informações Estratégicas de Defesa (SIED)	Lei Orgânica n.º 4/2014, de 13 de agosto - Diário da República, n.º 155, 1.ª Série, de 13 de agosto de 2014.Quinta alteração à Lei n.º 30/84, de 05 de setembro, que aprova a Lei Quadro do Sistema de Informações da República Portuguesa.
Segredo de Estado	Lei Orgânica n.º 12/2015, de 28 de agosto – Diário da República, n.º 168, 1.ª Série, de 28 de agosto de 2015.Alteração à Lei Orgânica n.º 3/2014, de 6 de agosto; cria Entidade Fiscalizadora Segredo de Estado.
Sistema Integrado das Redes de Emergência e Segurança de Portugal (SIRESP)	Resolução do Conselho de Ministros n.º 26/2002 de 05 de fevereiro. Posteriormente revogada pela RCM n.º 56/2003 de 08 de abril, Despacho n.º 16205/2005, de 26 de julho RCM n.º 74/2006 de 12 de junho
Aprovação das opções fundamentais do Sistema Integrado de Segurança Interna da República Portuguesa (SISI)	Resolução do Conselho de Ministros n.º 45/2007 de 19 de março.
Atividades de comércio e indústria de bens e tecnologias militares	Decreto-Lei n.º 56/2017, de 09 de junho – Diário da República, n.º 112, 1.ª Série, de 09 de junho de 2017.Altera (sexta alteração) a Lei n.º 37/2011, de 22 de junho, transpõe para ordem jurídica interna a Diretiva (UE) 2017/433, da Comissão, de 07Mar17.

Quadro 11 – Legislação nacional associada à área da segurança da informação

Tipo de Legislação	Identificação do documento legal
Lei das Comunicações Eletrónicas	Lei n.º 05/2004 de 10 de fevereiro.
Lei de Bases das Telecomunicações	Lei n.º 29/2002 de 06 de dezembro.
Lei do Cibercrime	Lei n.º 109/2009, de 15 de setembro. Transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Revoga a Lei n.º 109/91.
Regulamento Geral de Proteção de Dados	Lei n.º 58/2019, de 09 de agosto de 2019. Transpõe para a ordem jurídica interna o Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas (SEGNAC 1)	Resolução do Conselho de Ministros n.º 13/93, de 06 de março. Altera a RCM n.º 50/88, de 03 de dezembro.
Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Industrial, Tecnológica e de Investigação (SEGNAC 2)	Resolução do Conselho de Ministros n.º 37/1989 de 24 de outubro.
Instruções para a Segurança Nacional, Segurança das Telecomunicações (SEGNAC 3)	Resolução do Conselho de Ministros n.º 16/1994 de 22 de março.
Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática (SEGNAC 4)	Resolução do Conselho de Ministros n.º 16/1990 de 28 de fevereiro.
Comércio Eletrónico	Decreto-Lei n.º 7/2004 de 07 de janeiro
Práticas Comerciais Desleais	Decreto-Lei n.º 57/2008 de 26 de março
Utilização das plataformas eletrónicas de contratação pública	Lei n.º 96/2015, de 17 de agosto.
Sistema de Certificação Eletrónica do Estado - Infraestrutura de Chaves Públicas	Decreto-Lei n.º 116-A/2006, de 16 de junho. Designa a Autoridade Nacional de Segurança como autoridade credenciadora nacional (republicado).
Código Penal	Decreto-Lei n.º 48/95, de 15 de março – artigo 383.º.
Luta contra as formas graves de criminalidade	Lei n.º 20/2014, de 15 de abril. Estabelece normas de execução da decisão do Conselho UE que cria a EUROJUST e regula estatuto e competências do respetivo membro nacional.

Constituem ainda referências a considerar, os diplomas legais que, no âmbito do ordenamento jurídico nacional e europeu, procuram regulamentar a sociedade de informação, as comunicações e as áreas conexas que se lhe encontram associadas.

Apêndice H — Desenvolvimento integrado da capacidade de ciberdefesa

Processo Desenvolvimento de Capacidades (PDC)	Linha Estruturante	Objetivos	Resultados	Responsabilidade de coordenação	Relação com o planeamento de Defesa
OBJETIVOS: • Tornar as orientações para o desenvolvimento da CCDN, contidas na visão estratégica de longo prazo, mais específicas e por isso mais claras e úteis; • Identificar prioridades para o desenvolvimento de capacidades; • Identificar oportunidades de cooperação entre os atores envolvidos no PDC, qualquer que seja o seu âmbito (público ou privado, nacional ou internacional) ou tipo de solicitação (*top-down* ou *bottom-up*). **PERMITE ainda:** • Enquadrar e orientar os esforços de todos aqueles que participam no PDC; • Orientar atividades de ID&I e programas da indústria; • Definir métricas para avaliar a evolução do progresso da edificação da CCDN.	**Linha Estruturante A**	Identificar as lacunas de capacidades e avaliar o seu risco operacional, tendo em vista o estabelecimento da sua prioridade relativa face aos objetivos estratégicos (garantia da informação) a atingir no curto prazo (2019-2021).	• Base de referência para desenvolvimento e melhoria das capacidades necessárias para cumprir os objetivos da EMCIBER no curto prazo (Proteção da Redes das FFAA e condução de OpCiber); • Lista de lacunas de capacidades e lista de riscos resultantes das lacunas identificadas; • Orientação do MDN relativa às prioridades a seguir na gestão das lacunas; • Catálogo de requisitos e catálogo de recursos; • Relatório de progresso com priorização das lacunas identificadas (*input* para o processo de gestão de lacunas de capacidades).	• Ministério da Defesa Nacional; • EMGFA (papel apoio).	• Elaboração de Cenários; • Identificação de Missões no ciberespaço; • Nomenclatura e taxonomia das capacidades de ciberdefesa; • Estrutura de referência das capacidades; • Análise de lacunas egestão do risco (categorização e priorização).
	Linha Estruturante B	Determinar o impacto da visão estratégica de longo prazo no PDC.	• Tendências de evolução das tecnologias emergentes na área da ciberdefesa; • Lista de potenciais tendências de evolução da capacidade e características das missões e das operações a desenvolver no âmbito da componente operacional da EMCIBER no horizonte temporal 2025-2030; • Indicação de como um potencial risco (colocado por uma ameaça emergente no curto prazo) se pode desenvolver ao longo do tempo.	• Ministério da Defesa Naciona; • EMGFA (papel apoio).	• Análise estratégica; • Tendências de evolução das tecnologias associadas à ciberdefesa; • Tendências das capacidades ligadas à Defesa e ao planeamento de forças; • Plano ID&I ligado à ciberdefesa.
	Linha Estruturante C	Coligir em base de dados os projetos e planos de desenvolvimento de recursos (materiais e não-materiais), para identificar oportunidades de cooperação e sinergias no médio-longo prazo.	• Base de dados contendo uma listagem de todos os programas, projetos ou outras necessidades dos diversos atores envolvidos no desenvolvimento de capacidades de ciberdefesa (plano nacional e internacional); • Uma ferramenta que permitirá a avaliação global do desenvolvimento da área de capacidades de ciberdefesa desde o curto até ao longo prazo.	• Direção-Geral de Recursos da Defesa Nacional (DGRDN); • Ligação ao sistema de ID&I nacional e à base industrial de Defesa.	• Plano de reequipamento e modernização das FFAA; • Estratégia de ID&I das Indústrias de Defesa; • Ligação do plano ID&I de Defesa à Lei de Programação Militar.
	Linha Estruturante D	Identificar lições recolhidas da experiência em operações que poderão influenciar o futuro desenvolvimento de. capacidades.	• Análise das lições identificadas fornecendo dados relevantes para o Planeamento e melhoria das capacidades de ciberdefesa existentes; • Identificação de futuras tendências no desenvolvimento de capacidades.	• COCIBER/CNCS; • EMGFA (papel apoio).	• Identificação de alterações no emprego operacional de Forças e no tipo de Missões; • Tendências de evolução da capacidade de ciberdefesa.

PROJEÇÃO PARA O FUTURO

	Lista de tarefas a realizar	2019-2021	2022-2025	Até 2030
• Integração das quatro LE na implementação do PDC; • Desenvolvimento de ferramenta de apoio à gestão do PDC para ajudar o Ministério da Defesa Nacional e o EMGFA a lidar com a gestão das lacunas de capacidades; • Elaboração de lista de conclusões que serão na prática ações para dar seguimento ao trabalho do PDC (*e.g.*, novos projetos, estudo aprofundado de capacidades, investigação das novas necessidades de tecnologias, etc.).	• Elaborar uma lista genérica de tarefas baseada no conjunto de capacidades definidas no contexto da Estratégia Nacional de Ciberdefesa.	• Avaliação do risco a curto prazo, derivado da LE A, e influenciado pelas lições identificadas na LE D.	• Eventuais mudanças na avaliação do risco a médio prazo devido aos projetos em curso (LE C).	• Com base na informação da LE B (tendências para o futuro), projeta-se a forma como as capacidades vão ser influenciadas.

Fonte: Adaptado a partir de CDM (2003) e Nunes (2015, p.257)

Apêndice I — Avaliação dos vetores da capacidade de ciberdefesa nacional

Vetor de capacidade	Componente EMCIBER	Objetivos a atingir (EMGFA, 2019b)	Análise da situação atual Cf. ponto situação referido a 21 de janeiro de 2020 (EMGFA, 2020)	Nível de Maturidade	Impacto	Avaliação do impacto/ implicações
Doutrina	Operacional	Criar uma base doutrinária para a ciberdefesa a nível nacional, enquadrada pelo normativo das organizações a que Portugal pertence.	Elaborada uma proposta de ENCD (Out2019). Doutrina nacional para a ciberdefesa em consolidação (CCD e Ramos) – analisada doutrina NATO e dos EUA.	Médio/Baixo	Elevado	Edifício doutrinário para a ciberdefesa nacional, ainda em fase de consolidação; impõe limitações na continuidade dos processos; influencia reestruturação organizacional e edificação da capacidade.
Organização	Estrutural	Adequar a estrutura orgânica da ciberdefesa nacional e as suas relações organizacionais face às novas solicitações. Promover a representação e cooperação da ciberdefesa nacional.	Adotada estrutura orgânica base. Elaborada descrição de funções e qualificações como base para seleção de pessoal para o CCD (IOC-2021). Harmonização das estruturas dos Ramos. Identificados problemas em atingir quantitativos mínimos de pessoal. Participação do CCD em exercícios conjuntos - subsistem dificuldades em consolidar essa integração. CCD participa em diversos fóruns: G4 (CNCS, CCD, UNC3T e SIS), Grupo Ciber Resiliência do Instituto da Defesa Nacional (IDN) e Rede Comissão Interministerial de Política Externa - ameaças híbridas.	Baixa	Elevado	As dificuldades de integração e consolidação orgânica da estrutura de ciberdefesa, face às novas solicitações estratégicas, operacionais e doutrinárias (nacionais e NATO), poderá limitar bastante/impedir o natural desenvolvimento da capacidade de ciberdefesa das FFAA.
Treino	Operacional	Dinamizar sensibilização, educação e formação em ciberdefesa. Promover o treino coletivo e individual.	Desenvolvida plataforma para campanhas de sensibilização dos utilizadores dos domínios das FFAA e da Defesa. Estabelecidos contactos com empresas de formação–propostas em avaliação. Colaboração em diversas ações de formação (IDN, IUM, CNCS e NCI Academy). Promoção de ações de treino coletivo e individual-NATO (*Cyber Coalition*, *Locked Shields*, CWIX), 5+5 e nacional (Lusitano, CiberDEx e Ciber Perseu).	Médio/Baixo	Elevado	A formação, educação e treino especializado, desempenha um papel crucial tanto no desenvolvimento de competências dos quadros como na manutenção dos níveis de prontidão desejados/impostos pelas CNO. Subsiste a necessidade de identificar um perfil de competências, constituir um plano de formação e nivelar o ensino da ciberdefesa. – Fator condicionador do desenvolvimento da capacidade de ciberdefesa.
Material	Genética	Modernizar e sustentar os parques informáticos e as soluções tecnológicas da Defesa. Garantir a evolução futura das soluções tecnológicas para a ciberdefesa nacional.	Estabelecidos contactos com empresas e instituições do meio académico para avaliar ofertas de I&D nesta área e lançar desafios para o desenvolvimento de produtos e ferramentas inovadoras para a ciberdefesa.	Médio/Baixo	Médio	A transformação tecnológica e a adoção de novos conceitos emergentes e inovadores na área dos SIC e da ciberdefesa, impõe limitações na continuidade dos processos de reequipamento e influencia o desenvolvimento de capacidades.
Liderança	Operacional Estrutural	Satisfazer resposta estrutural e operacional da ciberdefesa nacional face aos desafios futuros, com o foco na gestão da mudança.	Participação em diversas conferências, eventos e atividades de promoção e sensibilização das lideranças para a ciberdefesa.	Baixo	Elevado	Ao nível da gestão de topo, a falta de sensibilização para a importância da cibersegurança e para o emprego operacional da ciberdefesa, impõe limitações à edificação da capacidade CNO.
Pessoal	Genética	Adequar a realidade dos RH afetos à ciberdefesa para os desafios futuros.	Constituição de grupo de trabalho (EPR: Divisão de Recursos/EMGFA, participação dos Ramos) para estudar propostas para a captação, sustentação e motivação dos quadros afetos à ciberdefesa das FFAA. Proposto modelo de formação especializada e aumento do período de exercício de funções técnicas na área da ciberdefesa – inamovibilidade 5 anos. Dificuldades na progressão vertical na carreira - satisfação condições especiais de promoção. Proposto modelo de carreira de progressão horizontal. Recrutamento nas FFAA e captação de talentos em universidades.	Médio/Baixo	Elevado	A reduzida quantidade de pessoal qualificado na área da ciberdefesa constitui uma lacuna crítica, condicionando decisivamente o processo de edificação desta capacidade. A inclusão de civis na estrutura de ciberdefesa das FFAA, numa primeira fase, só poderá ser concretizada com recurso às existências no âmbito da administração pública. A contratação de especialista será uma situação a contemplar no futuro, em função das necessidades a identificar.
Infraestruturas	Genética	Consolidar condições de utilização da capacidade de ciberdefesa nacional. Identificar infraestruturas para acomodar a nova organização a criar, sendo considerado o aproveitamento das já existentes.	Identificada a necessidade de adaptação e melhoria das infraestruturas atuais do CCD. Iniciado o processo administrativo relacionado com a empreitada a realizar. Fonte de financiamento identificada.	Média	Médio	As obras de adaptação das infraestruturas constituem um fator condicionador das condições de utilização da capacidade de ciberdefesa, permitindo criar condições para acomodar a nova organização a criar.
Interoperabilidade	Operacional	Dinamizar os processos de interoperabilidade da ciberdefesa com atores externos.	Utilização de ferramenta comum de partilha de informação de ciberdefesa (EMGFA e Ramos) e cibersegurança (CCD, CNCS e SIS). Participação em exercícios nacionais e internacionais. Envolvimento em fóruns internacionais e em projetos e grupos de trabalho ao nível NATO e da UE (projetos PESCO).	Média	Médio	O nível de interoperabilidade deverá ser reforçado na sua máxima extensão. Não apresenta neste momento impacto visível na edificação da capacidade.

Apêndice J — Caracterização da envolvente da capacidade de ciberdefesa

Como resultado da análise da envolvente em que decorre a edificação da CCDFFAA (Quadros 12 e 13), conforme percecionada ao nível dos seus vectores de capacidade (DOTMLPII), apresenta-se neste apêndice uma caracterização do seu ambiente interno (potencialidades e vulnerabilidades) e externo (oportunidades e ameaças). Neste contexto, salienta-se o facto de na análise do ambiente externo ter sido realizada uma análise Política, Económica, Social, Tecnológica, Ambiental e Legal (PESTAL). Foram incluidos nesta análise os resultados do trabalho elaborado pelo Grupo de Trabalho-Capacidade de Ciberdefesa das Forças Armadas (EMGFA, 2019b).

Quadro 12 – Resultado da análise interna (potencialidades e vulnerabilidades)

Vetor Capacidade	Potencialidades (*Strengths*)	Vulnerabilidades (*Weaknesses*)
Doutrina	Doutrina técnico-tática multissectorial.	Doutrina limitada ou desarticulada.
Organização	Existência de uma estrutura-base para a ciberdefesa edificada (CCD).	Estrutura orgânica atual (CCD) inadequada face às novas solicitações.
		Integração da componente de ciberdefesa nas operações conjuntas – não se verifica.
		C2 da ciberdefesa – não integrado, heterogéneo e limitado junto dos Ramos.
Treino	Oportunidades de treino operacional.	Plataformas de treino (coletivo e individual).
	Integração do ciberespaço no exercício conjunto (Lusitano).	Ciberdefesa não integrada na formação de base dos quadros (Academias).
	Reconhecimento internacional da capacidade em exercícios.	Formação técnica especializada – limitada, dispendiosa e longa.
		Sensibilização para a cibersegurança na Defesa Nacional (cyber a*wareness*) – limitada.
Material	Financiamento disponível para o desenvolvimento da capacidade	Ferramentas de monitorização – cobertura nacional limitada/deficitária.
	Capacidades baseadas em plataformas tecnológicas edificadas	Parte do parque informático das FFAA obsoleto / sem suporte.
Liderança	Compromisso da estrutura de topo para desenvolvimento da capacidade.	Desconhecimento estratégico da utilização da capacidade cibernética.
	Vontade demostrada de apostar na capacitação dos RH.	Dificuldades em transmitir a necessidade de ser adotada uma aproximação holística à ciberdefesa.
		Dificuldade de operacionalização do novo domínio.
Pessoal	Inamovibilidade dos quadros - período de 5 anos (na 1.ª colocação no CCD).	Mecanismos de captação e retenção de pessoal externo às FFAA – inexistência.
	Mecanismo de fixação dos militares à carreira militar.	Gestão de carreiras do pessoal técnico - impacto da inamovibilidade na carreira dos militares.
	Valorização dos RH das FFAA.	Gestão de carreiras - falta de regulamentação
Infraestruturas	Infraestruturas de operação adequadas face às necessidades atuais.	Atuais instalações do CCD não comportam aumento planeado dos RH e das áreas técnicas.
	Infraestrutura dos Ramos- Núcleos CIRC.	
Interoperabilidade	Protocolos de cooperação com entidades externas.	Relutância das nações / organizações na partilha de vulnerabilidades, comprometimentos e soluções.

Fonte: Adaptado a partir de EMGFA (2019b, pp. 16-17).

Quadro 13 – Resultado da análise externa (oportunidades e ameaças)

Vetor Capacidade	Oportunidades (*Opportunities*)	Ameaças (*Threats*)
Doutrina	Doutrina NATO (OpCiber) disponível e participação nacional no CCDCOE.	Diferentes abordagens nacionais limitam entendimento geral para uma doutrina comum (NATO).
Organização	Existência de diversos organismos, setor público/privado, ligados ao ciberespaço.	Potenciais adversários (estatais e não-estatais) possuem estruturas organizadas e ágeis na adaptação ao ambiente.
		Aparecimento de novas ameaças de atores Estado e não-Estado (terrorismo, *hacktivismo*, corporações, etc.).
Treino	Projeto MNCDE&T liderado por PT e colideranca do *Cyber Discipline* da UE.	Formação técnica especializada de duração extensa e custos elevados.
	Edificação do CAIH na Academia Militar e da *NCI Academy* (Oeiras).	
	Existência de formação geral nas áreas da cibersegurança em Portugal.	
Material	Novas tecnologias com aplicabilidade na ciberdefesa (possibilidade de automatizar processo resposta a incidentes, inclui IA).	Espetro de ciberameaças complexo, com rápida evolução e sofisticação, não sendo este processo sempre acompanhado pelas soluções de segurança adequadas.
		Utilização crescente ciberespaço de natureza assimétrica.
Liderança	Alinhamento de vontades nacionais e internacionais com maior financiamento de projetos na área da ciberdefesa.	Assimetrias tecnológicas, financeiras e de RH entre nações.
	Procura crescente da criação de sinergias Nacionais e Cooperação Internacional.	Insuficientes parcerias com entidades públicas e privadas limitam aproximação interagência.
	ENSC 2019 -2023 (V2.0).	
	Ciberespaço – Novo domínio Operações.	
Pessoal	Vontade de integrar a componente de ciberdefesa das FFAA.	Captação RH especializados a curto/médio prazo, depende de alterações legislativas para garantir suporte orçamental.
		Processos de captação de RH a longo prazo pendente; reestruturação da formação de base dos militares, e criação de mecanismos para a gestão das carreiras.
		Falta de perfis de carreiras com a respetiva formação.
		RH reduzidos – Indústria oferece melhores condições.
Interoperabilidade	Partilha de informação com Aliados.	Dificuldades na partilha de informação e na cooperação operacional no combate a ameaças sofisticadas, complexas híbridas e dissimuladas.

Fonte: Adaptado a partir de EMGFA (2019b, pp. 23-24).

Apêndice K — Objetivos estratégicos e linhas de ação da CCDN

Vetor Capacidade	EMCIBER	Objetivos Estratégicos Estruturantes		Linhas de Ação		EPR	Decisão	Prazo	Observação
Doutrina	**Genética**	**OEE 9**	Criar um edifício doutrinário para a ciberdefesa (nível nacional), tendo como referência as organizações internacionais a que Portugal pertence.	9.01	Elaborar a doutrina estratégica da ciberdefesa	DIPLAEM	CCEM	Out19	Atraso
				9.02	Elaborar a doutrina operacional para a ciberdefesa	COCIBER	CEMGFA	Jun20	Em curso
				9.03	Elaborar a doutrina tática para a ciberdefesa	COCIBER	CEMGFA	Mar21	
				9.04	Elaborar normas e regras de empenhamento para condução de OpCiber	CCOM	MDN	Jun21	
Organização	**Estrutural**	**OEE 6**	Adequar a estrutura orgânica da ciberdefesa nacional e a sua integração orgânica face às novas solicitações.	6.01	Propor uma estrutura orgânica para o COCIBER	COCIBER	CEMGFA	Mai19	Atraso
				6.02	Otimizar a estrutura dos núcleos CIRC dos Ramos, EMGFA e Defesa	COCIBER	CEMGFA+MDN	Jul19	Atraso
				6.03	Consolidar a relação do COCIBER com o CISMIL	COCIBER	CEMGFA	Out20	
				6.04	Integrar a componente cibernética nas operações conjuntas	COCIBER	CEMGFA	Abr20	Atraso
	Operacional	**OEE 12**	Garantir a condução eficiente e eficaz de CNO, alinhando a resposta genética e operacional da ciberdefesa	12.01	Reforçar capacidade de *Computer Network Defence*	COCIBER	CEMGFA	Jun20	Em curso
				12.02	Incrementar capacidade *Computer Network Exploitation*	COCIBER	CEMGFA	Jan21	
				12.03	Desenvolver capacidade *Computer Network Attack*	COCIBER	CEMGFA	Jun21	
	Estrutural	**OEE 7**	Promover a representação e cooperação da ciberdefesa nacional.	7.01	Promover a representação da ciberdefesa em organismos nacionais	COCIBER	CEMGFA	Set19	
				7.02	Dinamizar a cooperação com o setor público e privado	COCIBER	CEMGFA	Continuo	
				7.03	Potenciar a cooperação com os aliados e organizações internacionais	COCIBER	CEMGFA+MDN	Continuo	
				7.04	Promover criação de um órgão (nível do CSDC) para acompanhar plano de ação ENSC 2.0	COCIBER	CEMGFA	Aprovar	Aguardar
Treino	**Operacional**	**OEE 05**	Promover a sensibilização, educação e formação em ciberdefesa.	5.01	Elaborar plano de formação do COCIBER	COCIBER	CEMGFA	Mai19	
				5.02	Adaptar planos de formação dos estabelecimentos de ensino militares (área da ciberdefesa)	IUM	CEMGFA	Dez19	Atraso
				5.03	Promover envolvimento dos diferentes níveis da Defesa no esforço contínuo de sensibilização	COCIBER	MDN	Nov19	Atraso
				5.04	Elaborar protocolos bilaterais para potenciar a formação – foco áreas técnicas e CNO	COCIBER	CEMGFA	Continuo	
		OEE 10	Potenciar o treino coletivo e individual.	10.01	Dinamizar o treino coletivo e individual	COCIBER	CEMGFA	Continuo	
				10.02	Apoiar a realização de cursos através de formadores do COCIBER	COCIBER	CEMGFA	Continuo	
Material	**Genética**	**OEE 1**	Modernizar e sustentar os parques informáticos e as soluções tecnológicas das redes da Defesa Nacional.	1.01	Consolidar os parques informáticos das redes da Defesa Nacional	DIRCSI	CEMGFA+CEM	Dez19	Atraso
				1.02	Harmonizar as soluções tecnológicas das redes da Defesa Nacional	DIRCSI	CEMGFA+CEM	Dez20	
				1.03	Integrar todos os ativos das redes da Defesa Nacional nas plataformas de monitorização	COCIBER	CEMGFA	Dez21	
	Genética	**OEE 4**	Dinamizar a evolução futura das soluções tecnológicas para a ciberdefesa nacional.	4.01	Estudar, propor e adquirir plataformas de treino individual e coletiva	COCIBER	CEMGFA	Dez19	Atraso
				4.02	Elaborar um plano de sustentação da infraestrutura tecnológica da ciberdefesa	COCIBER	CEMGFA	Set20	
				4.03	Garantir a atualização tecnológica das plataformas da capacidade de ciberdefesa	COCIBER	CEMGFA	Continuo	
				4.04	Fortalecer sinergias com a indústria e academia na procura de novas soluções tecnológicas	COCIBER+DGRDN	CEMGFA	Continuo	
Liderança	**Genética**	**OEE 3**	Alinhar a resposta estrutural e operacional da ciberdefesa nacional face aos desafios futuros.	3.01	Garantir o processo de gestão estratégica da mudança	DIPLAEM	CEMGFA	Continuo	
				3.02	Garantir as fontes de financiamento adequadas para o desenvolvimento da capacidade	DIPLAEM	CEMGFA	Continuo	
				3.03	Promover a liderança nacional em iniciativas internacionais	COCIBER	CEMGFA+MDN	Continuo	
Pessoal	**Genética**	**OEE 8**	Adequar a realidade dos RH afetos à ciberdefesa aos desafios futuros.	8.01	Gerir carreiras	DIREC	MDN	Continuo	
				8.02	Obter RH	DIREC	MDN	Dez19	Atraso
				8.03	Manter efetivos	DIREC	MDN	Continuo	
Infraestruturas	**Genética**	**OEE 2**	Consolidar infraestruturas e condições de utilização da capacidade da ciberdefesa nacional.	2.01	Identificar infraestruturas necessárias para acomodar o COCIBER (capacidades requeridas)	COCIBER	CEMGFA	Jul20	
				2.02	Aproveitar a utilização de infraestruturas externas ao COCIBER	COCIBER	CEMGFA	Continuo	
Interoperabilidade	**Operacional**	**OEE 11**	Consolidar processos de interoperabilidade da ciberdefesa com atores externos.	11.01	Otimizar o processo de partilha de informação ao nível da Defesa	COCIBER	MDN	Dez21	
				11.02	Dinamizar a partilha de informação	COCIBER	CEMGFA	Continuo	
				11.03	Dinamizar o intercâmbio de RH	COCIBER	CEMGFA	Continuo	

Fonte: Adaptado a partir de EMGFA (2019b).