INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE PROMOÇÃO A OFICIAL SUPERIOR
2020/2021 – 2.ª Edição

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

EDIFICAÇÃO DE UM RAMO INDEPENDENTE DAS FORÇAS ARMADAS PARA O DOMÍNIO DO CIBERESPAÇO

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 OU DA GUARDA NACIONAL REPUBLICANA.

Rodrigo Serrano dos Santos
1TEN, EN-AEL

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

EDIFICAÇÃO DE UM RAMO INDEPENDENTE DAS FORÇAS ARMADAS PARA O DOMÍNIO DO CIBERESPAÇO

1TEN, EN-AEL Rodrigo Serrano dos Santos

Trabalho de Investigação Individual do CPOS M 2020/2021 – 2.ª Edição

Pedrouços 2021

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

EDIFICAÇÃO DE UM RAMO INDEPENDENTE DAS FORÇAS ARMADAS PARA O DOMÍNIO DO CIBERESPAÇO

1TEN, EN-AEL Rodrigo Serrano dos Santos

Trabalho de Investigação Individual do CPOS M 2020/2021 – 2.ª Edição

Orientador: TCOR, ENGEL Pedro Miguel da Silva Costa

Pedrouços 2021

Declaração de compromisso Antiplágio

Eu, **Rodrigo Serrano dos Santos**, declaro por minha honra que o documento intitulado **Edificação de um Ramo independente das Forças Armadas para o domínio do ciberespaço** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Promoção a Oficial Superior 2020/2021 – 2.ª Edição** 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**, 12** de **julho** de **2021**

Rodrigo Serrano dos Santos

Assinado por : **Rodrigo Serrano dos Santos**
Num. de Identificação: 13113074
Data: 2021.07.27 15:43:18+01'00'

CHAVE MÓVEL

Agradecimentos

Para a realização deste trabalho de investigação, foi indispensável o apoio e colaboração de diversas pessoas que duma forma ou de outra, constituíram o suporte que ajudou à sua concretização.

Um enorme agradecimento ao meu orientador, Tenente-coronel Silva Costa, pela sua permanente orientação e disponibilidade, pelas suas sugestões e comentários, e pelo grande apoio prestado na definição da abordagem ao tema, que em muito contribuíram para a prossecução dos objetivos e conclusão do presente trabalho.

Agradeço a todos os entrevistados, que demonstraram inteira disponibilidade para colaborar neste trabalho, dando um contributo fundamental para a o seu enriquecimento e concretização.

Aos camaradas do Curso de Promoção a Oficial Superior 2020/2021 – 2.ª Edição, pela amizade e camaradagem revelada durante o curso.

Agradeço à minha família, e em especial à minha esposa Catarina, que formam um forte alicerce para alcançar os meus objetivos, através do amor, força, paciência, apoio, determinação e incentivo, sem o qual, certamente tudo seria mais difícil de alcançar.

A todos aqueles que de forma direta ou indireta
contribuíram para a realização deste trabalho,
o meu muito obrigado.

Índice

Índice de Apêndices

Índice de Figuras

Resumo

Encontramo-nos numa era em que a digitalização e a diluição de fronteiras por via da globalização, representam na área da segurança, a necessidade de uma urgente e profunda reflexão, pois enfrentamos ameaças cada vez mais sofisticadas, que colocam em risco a soberania da nação. Com a emergente relevância que o ciberespaço teve na última década, e elevada importância que este possa vir a ter no domínio da segurança e Defesa, Portugal, deverá promover a edificação de uma capacidade de ciberdefesa robusta e capaz de fazer face aos desafios no ciberespaço.

O presente trabalho visa caracterizar a capacidade militar atual das Forças Armadas Portuguesas para atuar no domínio do ciberespaço, e identificar contributos para a criação de um modelo de capacitação militar com capacidade de atuar no ciberespaço, integrando também tudo o que é comum no quadro dos sistemas de informação e comunicações.

Para elaboração desta investigação, assumiu-se uma orientação ontológica construtivista e uma orientação epistemológica interpretativa, fazendo uso de um raciocínio indutivo, através de uma estratégia qualitativa baseada num estudo de caso do objeto da investigação, com recurso à análise documental e dados recolhidos nas entrevistas a especialistas ligados à cibersegurança e ciberdefesa nacional.

Dos resultados obtidos, recomenda-se a centralização da ciberdefesa e das Tecnologias da Informação e Comunicações no Estado-Maior-General das Forças Armadas, numa perspetiva de racionalização de recursos, economia de escala e uniformização da infraestrutura das Forças Armadas, uma vez que, a edificação de um Ramo independente das Forças Armadas com capacidade para aturar no domínio do ciberespaço é considerada como não adequada a curto/médio prazo pelos especialistas entrevistados, embora estes reconheçam que se deva dar passos na direção da capacitação da ciberdefesa nacional, de modo a que eventualmente possa ser alcançado um Ramo independente a médio/longo prazo.

Este processo de capacitação da ciberdefesa, permitirá às Forças Armadas defender as suas redes de forma mais eficiente e eficaz contra ciberataques, e realizar operações militares no ciberespaço, contribuindo para que Portugal disponha de uma capacidade mais robusta e mais credível para assegurar a ciberdefesa nacional.

Palavras-chave: Capacidade Militar, Ciberdefesa, Ciberespaço, Forças Armadas, Racionalização de Recursos.

Abstract

We live in an era where digitization and the borderless world effect due globalization represent, in security, the need for an urgent and profound reflection, as we face increasingly sophisticated threats, which put the nation sovereignty at risk. With cyberspace emerging relevance in the last decade, and the high importance that it may have in security and defense, Portugal should promote a robust cyber defense capability, capable of facing the upcoming cyberspace challenges.

The goal of this study is to characterize the current Portuguese armed forces capability to operate in cyberspace domain and identify contributions to build a military model to act in cyberspace, integrating everything that is common within the information and communications systems.

In the development of this investigation was used a constructivist ontological orientation and an interpretive epistemological orientation, with an inductive reasoning, through a qualitative strategy based on a case study of the object of investigation, by means of document analysis and interviews with cybersecurity and cyber defense experts.

Based on the obtained results, it is recommended the centralization of cyber defense and Information and Communications Technologies in the General Staff of the Armed Forces, from the perspective of rationalization of resources, economy of scale and standardization of the infrastructure of the Armed Forces. Despite, the edification of an independent Branch of the Armed Forces capable to act in the domain of cyberspace is considered not adequate in the short/medium term by the interviewed experts, they recognize that should be taken steps to increase the capability of national cyber defense, in order to eventually be created an independent branch in the medium/long term.

This cyber defense capacity building process will allow the Armed Forces to defend their networks more efficiently and effectively against cyberattacks, and carry out military operations in cyberspace, contributing to a stronger and more credible capacity to ensure Portuguese national cyber defense.

***Keywords**: Military Capability, Cyber Defense, Cyberspace, Armed Forces, Resource Rationalization.*

Lista de abreviaturas, siglas e acrónimos

C

CCD	Centro de Ciberdefesa
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CCOM	Comando Conjunto para as Operações Militares
CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CIDS	*Cyber and Information Domain Service*
CIRC	*Computer Incident Response Capability*
CISIO	*Communication and Information Systems Infrastructure Operations*
CISRO	*Cyberspace Information Surveillance and Reconnaissance Operations*
CNCS	Centro Nacional de Cibersegurança
CONOPS	Conceito de Operações
CPLP	Comunidade dos Países de Língua Portuguesa
CSIRT	*Computer Security Incident Response Team*
CUE	Conselho da União Europeia
CWIX	*Coalition Warrior Interoperability eXercise*
CYOC	*Cyberspace Operations Centre*

D

DCSI	Direção de Comunicações e Sistemas de Informação
DIRCSI	Direção de Comunicações e Sistemas de Informação
DITIC	Direção de Tecnologias da Informação e Comunicações
DOD	*Department of Defense*
DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade
DR	Decreto Regulamentar

E

EC	*European Commission*
EMA	Estado-Maior da Armada

EMGFA	Estado-Maior-General das Forças Armadas
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EU	*European Union*

F

FA	Força Aérea
FFAA	Forças Armadas
FMN	*Federated Mission Networking*

G

GT-CCFA	Grupo de Trabalho para o desenvolvimento da Capacidade de Ciberdefesa das Forças Armadas

I

IP	*Internet Protocol*

L

LPM	Lei de Programação Militar

M

MDN	Ministério da Defesa Nacional

N

NATO	*North Atlantic Treaty Organization*
NCIRC	Núcleo de Computer Incident Response Capability

O

OE	Objetivos Específicos
OG	Objetivo Geral
OODA	*Loop Observ, Orient, Decide and Act*
OPTASK	Operational Tasking
OTAN	Organização do Tratado do Atlântico Norte (NATO - *North Atlantic Treaty Organization*)

P

PE	Parlamento Europeu
PRTCERTDEF	Centro de Operações do Centro de Ciberdefesa

Q

QC	Questão Central
QD	Questões Derivadas

R

RCM	Resolução do Conselho de Ministros

S

SGMDN	Secretaria-Geral do Ministério da Defesa Nacional
STI	Superintendência das Tecnologias da Informação
SWOT	Forças, Fraquezas, Oportunidades e Ameaças

T

TIC	Tecnologias da Informação e Comunicações
TII	Trabalho de Investigação Individual

U

EU	União Europeia (*EU - European Union*)
USCYBERCOM	*United States Cyber Command*

1. Introdução

Os desafios atuais da cibersegurança representam o início de uma era tecnológica, em que os ciberataques estimulam que adversários potencialmente mais fracos possam superar um poder militar convencional superior de forma instantânea e difícil de rastrear, colocando em risco a soberania da nação (Lynn III, 2010).

> *The tactics and leadership necessary in cyber are distinct and different. This is true down through the ranks as well. Cyber is not just another support military job, like supply or maintenance. It is a significant weapon of strike and shield of defense [...]* (Forsling, 2016)

Por norma, estes ataques não causam baixas em massa, como os ataques tradicionais, mas têm potencial de exfiltrar propriedade intelectual, permitindo ganhar vantagem económica no mercado global, restringir a operacionalidade de sistemas e serviços, ou até mesmo paralisar uma nação (Lynn III, 2010).

Neste contexto, em 2014 na cimeira de Gales, a Organização do Tratado do Atlântico Norte (OTAN) declarou a ciberdefesa como parte central da missão de defesa coletiva da Aliança, tendo em 2016 na cimeira de Varsóvia, declarado o ciberespaço como um domínio de operações militares.

> *At the Warsaw Summit in July 2016, Allied Heads of State and Government reaffirmed NATO's defensive mandate and recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. […] Allies also committed through a Cyber Defence Pledge to enhancing the cyber defences of their national networks and infrastructures, as a matter of priority. Each Ally will honour its responsibility to improve its resilience and ability to respond quickly and effectively to cyber attacks, including as part of hybrid campaigns. (OTAN, 2020b)*

De igual forma, em 2018, a União Europeia (UE) também identificou o ciberespaço como sendo um domínio de operações.

> *In 2018, the EU identified cyberspace as a domain of operations […] The EU and Member States should provide further impetus for the development of state-of-the-art cyber defence capabilities […] the EU should further foster cooperation among Member States on cyber defence research, innovation and capability development.* (*European Commission* [EC], 2020a)

Ambas as organizações identificaram ainda como necessidade primária, investir no incremento da capacidade de ciberdefesa própria e dos estados-membros, bem como no aumento da resiliência a ciberataques através da implementação de estratégias de cibersegurança.

Com a emergente relevância que o ciberespaço teve na última década, e elevada importância que a OTAN e a UE admitem que este possa vir a ter para acompanhar a evolução e obter vantagem em futuras operações militares, Portugal como membro destas organizações, deverá promover a edificação de uma capacidade de ciberdefesa robusta e capaz de fazer face aos desafios no ciberespaço (Ministério da Defesa Nacional [MDN], 2013).

Em 2015, ainda antes da OTAN e UE declararem o ciberespaço como um domínio de operações, Portugal já tinha promulgado a Estratégia Nacional de Segurança do Ciberespaço (ENSC), com vista a garantir a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço. Esta Estratégia foi revista algumas vezes ao longo dos anos, para acomodar as diretivas da OTAN e da UE. Encontra-se atualmente em vigor a ENSC 2019-2023, aprovada em 23 de maio de 2019, que reitera a elevada importância do ciberespaço e da capacidade de ciberdefesa para garantir a soberania nacional.

> *Desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional.* (Resolução do Conselho de Ministros [RCM], 2019)

O presente Trabalho de Investigação Individual (TII) tem por objeto de estudo a avaliação da adequabilidade de edificação de um Ramo independente das Forças Armadas (FFAA), com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações, e encontra-se delimitado pelos seguintes domínios, conforme preconizado por Santos & Lima (2019, p. 44):

- Temporal, tem como termo de referência de início a RCM n.º 26/2013, de 19 de abril, onde foi definida a orientação estratégica para a ciberdefesa, no quadro da reforma "Defesa 2020", e como termo de referência final, o período da realização deste estudo, julho de 2021.

- Espacial, centrar-se-á nas FFAA Portuguesas e no seu relacionamento com a estrutura nacional de segurança do ciberespaço, com especial enfoque na relação da componente militar (ciberdefesa), com o nível estratégico, e com a componente civil (cibersegurança).

- Concetual, cingir-se-á à realização de entrevistas a especialistas, e à análise da legislação nacional, da OTAN e da UE que contribui para o quadro legal em vigor no domínio do ciberespaço.

Como Objetivo Geral (OG), este TII pretende avaliar a adequabilidade de edificação de um Ramo independente das FFAA, com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações. De modo a contribuir para alcançar este OG, a investigação visa responder à Questão Central (QC): "Será adequado edificar um Ramo independente das FFAA com capacidade para aturar no domínio do ciberespaço?".

A importância e atualidade do tema para o contexto nacional da ciberdefesa, de acordo com o enquadramento apresentado, revestem o presente TII de especial importância, interesse e relevância, esperando-se ainda que possa vir a ser um significativo contributo para as FFAA e, consequentemente, para a Defesa Nacional.

Este TII encontra-se organizado em cinco capítulos, sendo o primeiro a introdução. O segundo capítulo apresenta o enquadramento teórico, conceptual e metodológico, e o modelo de análise. No terceiro capítulo far-se-á a análise da atual capacidade e modelo orgânico das FFAA para atuar no domínio do ciberespaço, enquanto no quarto capítulo ir-se-á propor um modelo de edificação da capacidade nacional de operação no ciberespaço, identificando as suas forças, fraquezas, oportunidades e ameaças. Este capítulo visa ainda responder à QC, seguindo-se o capítulo das conclusões, onde serão resumidos os resultados, realçados contributos para o conhecimento e identificadas possíveis investigações futuras.

2. Enquadramento

Neste capítulo será apresentado o enquadramento teórico, onde serão descritos os conceitos estruturantes do domínio do ciberespaço, o modelo de análise e a metodologia.

2.1 Enquadramento conceptual

Através da revisão de literatura, do quadro jurídico em vigor, e compromissos nacionais assumidos com os parceiros estratégicos, serão descritos neste capítulo os conceitos estruturantes para o domínio do ciberespaço.

2.1.1 Ciberespaço

Não existe uma definição única e inequívoca do domínio do ciberespaço, uma vez que ao contrário do domínio do mar, terra e ar, o ciberespaço é uma criação do homem, não é tangível, e é transversalmente dependente dos outros domínios de operações.

De modo a melhor compreender o ciberespaço, a *Joint Publication 3-12: Cyberspace Operations* (2018) define-o como sendo o domínio dentro do ambiente da informação que consiste na interdependência das infraestruturas de rede das tecnologias da informação e dos dados residentes. Esta definição engloba a Internet, redes de telecomunicações, sistemas computorizados, e todo o tipo de processadores e controladores.

Nessa publicação, é ainda possível identificar um modelo de representação do ciberespaço em termos de três camadas interrelacionadas: camada física, camada lógica e a camada das ciber-pessoas, conforme Figura 1.

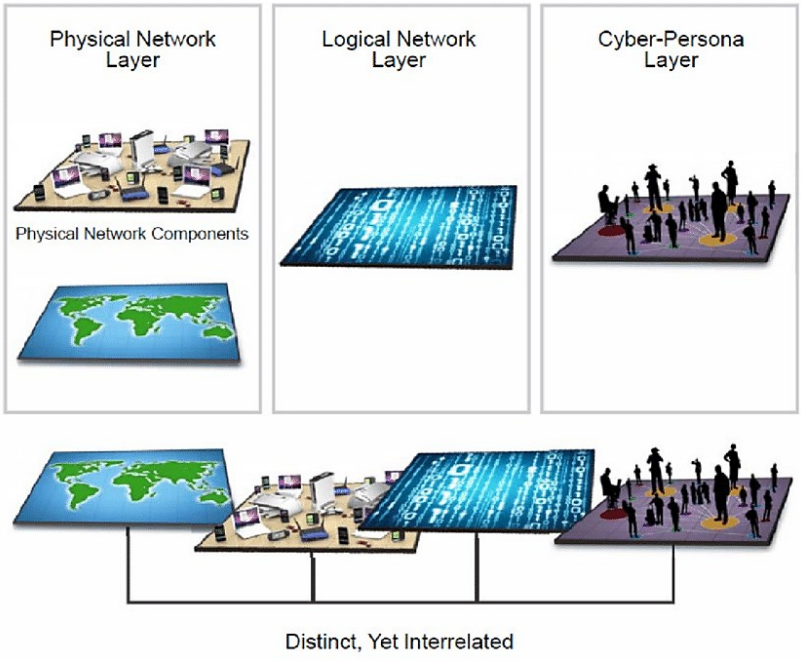

Figura 1 - Camadas que compõem o ciberespaço

Fonte: *United States Cyber Command* (USCYBERCOM) (2018, pp. I-3).

A camada física consiste nos equipamentos de tecnologias de informação e nas infraestruturas que fornecem o armazenamento, transporte e processamento de informação. Por sua vez, a camada de rede consiste na forma como os diversos elementos estão relacionados e trocam informação entre si. Nesta camada, vários nós da camada física que concorrem para o mesmo propósito podem ser representados como apenas um elemento de rede. Por fim, a camada das ciber-pessoas proporciona uma visão do ciberespaço criada pela abstração dos dados da camada de rede lógica, permitindo representar digitalmente a identidade de um ator ou entidade no ciberespaço, a ciber-pessoa. Nesta camada encontram-se os utilizadores, que podem ser personificados de acordo com um conjunto de identificadores, tais como os seus dados pessoais ou organizacionais, endereços de protocolo da internet (IP), endereços de e-mail, ou relacionamentos no ciberespaço, entre outros. Sendo que esses utilizadores podem, ou não, estar diretamente associados a pessoas ou entidades reais (USCYBERCOM, 2018).

A camada das ciber-pessoas encontra-se revestida de enorme complexidade, uma vez que um único indivíduo pode criar e manter múltiplas ciber-pessoas através da utilização de múltiplos identificadores no ciberespaço, ou mesmo vários indivíduos podem partilhar um mesmo indicador, como por exemplo uma conta de utilizador ou endereço de IP. Além disso, os elementos desta camada podem encontrar-se em várias localizações virtuais que não se encontram vinculadas a uma única localização física. Desse modo, a sua identificação requer uma significante recolha e análise de dados de inteligência para ser possível identificar uma ameaça de forma efetiva, ou para alcançar o efeito desejado. Tal como acontece na camada lógica, alterações complexas na camada das ciber-pessoas podem acontecer muito rapidamente, em comparação com as alterações semelhantes na camada física, tornando as ações contra essas ameaças bastante complexas (USCYBERCOM, 2018).

2.1.2 Estratégia de operação no domínio do ciberespaço

Caraterizado o ciberespaço como um domínio diferenciado, importa compreender a estratégia de operação neste domínio adotada por Portugal, bem como a estratégia adotada pela OTAN e pela UE, que desde 2016 cooperam na prevenção e resposta a ciberataques, e que são as principais referências de Portugal, como país membro de ambas as organizações.

2.1.2.1 Organização do Tratado do Atlântico Norte

A abordagem da OTAN relativamente à ciberdefesa evoluiu significativamente nos últimos 20 anos, como podemos ver na Figura 2, reforçando a sua importância como um

elemento que pode contribuir substancialmente para a defesa coletiva, gestão de crises e segurança cooperativa.

Figura 2 - Cronologia OTAN

Em particular, foi reconhecido em 2014 que o potencial de um ciberataque é equiparável ao de um ataque armado, tendo sido aprovada a capacidade de invocar o artigo 5º do tratado de Washington, para permitir uma defesa cooperativa, caso um país da Aliança seja alvo de um ciberataque (OTAN, 2014).

A OTAN encontra-se intrinsecamente ligada ao domínio digital e às ameaças que este representa para si e para os estados-membros, uma vez que o ciberespaço é um domínio internacional por natureza. Desde 2014 que a OTAN afirma a ciberdefesa como parte central da missão de defesa coletiva da Aliança, tendo declarado o ciberespaço como um domínio de operações militares no decorrer de 2016, identificando ainda a necessidade de investir no incremento da capacidade de ciberdefesa própria e dos estados-membros, na resiliência a ciberataques, e implementação de estratégias de cibersegurança (OTAN, 2020b).

O reconhecimento do ciberespaço como domínio de operações foi um marco importante para a capacitação da OTAN e dos seus aliados, no entanto, no que concerne aos aliados, a estrutura da OTAN serve principalmente de suporte ao processo de decisão, mantendo cada país a sua própria liderança político-militar para o ciberespaço (Marrone & Sabatino, 2021).

2.1.2.2 União Europeia

A UE declarou o ciberespaço como o quinto domínio de operações em 2018, quando efetuou a revisão do Quadro Estratégico da UE para a ciberdefesa (ver Figura 3), afirmando que o êxito das missões e operações no ciberespaço dependem cada vez mais de um ciberespaço seguro e resiliente, para o qual todos os estados-membros devem contribuir (Conselho da União Europeia [CUE], 2018).

Figura 3 - Cronologia UE

A Estratégia da UE para a cibersegurança promulgada em 2013 foi o primeiro ato legislativo da UE para o domínio do ciberespaço, e tem como principal destinatário os estados-membros. Esta estratégia identifica que os sistemas de informação e a Internet desempenham um papel fundamental na circulação transfronteiriça de mercadorias, serviços e pessoas. Por conseguinte, a segurança das redes e dos sistemas de informação torna-se essencial para o bom funcionamento do mercado interno europeu. Desse modo, essa estratégia propõe a criação de um mecanismo de cooperação e partilha que permita uma eficaz resposta a incidentes de segurança nas redes e nos sistemas de informação dos estados-membro (EC, 2013).

Em 2016, a diretiva da UE 2016/1148, estabelece a obrigação dos estados-membros designarem autoridades nacionais competentes, pontos de contato únicos e *Computer Security Incident Response Team* (CSIRT) responsáveis por resolver incidentes relacionados

com a segurança das redes e dos sistemas de informação, para criar uma rede de equipas de resposta a incidentes que permita desenvolver a confiança entre estados-membros e promover uma cooperação operacional célere e eficaz (Parlamento Europeu [PE], 2016).

Mais recentemente, em 2019, a UE desenvolveu um sistema europeu de certificação, com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, serviços e processos de tecnologias de informação e comunicação na UE, e evitar a fragmentação do mercado interno no que respeita aos sistemas de certificação de cibersegurança (PE, 2019).

Por fim, a nova Estratégia Europeia de Cibersegurança apresentada em dezembro de 2020, visa aumentar a resiliência e soberania tecnológica dos estados-membros e da UE, bem como investir na capacidade operacional para prevenir, dissuadir e responder a ameaças no ciberespaço, tornando o ciberespaço global e aberto, por via de uma maior cooperação (EC, 2020b).

2.1.2.3 Portugal

Ao longo dos últimos anos, tendo como linhas orientadoras as diretivas da OTAN e da UE, Portugal tem vindo a desenvolver um conjunto de medidas, como podemos observar na Figura 4, com vista a garantir uma utilização livre e segura do ciberespaço por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas. Em 2008, Portugal adaptou ao direito nacional a Convenção sobre Cibercrime do Conselho da Europa, tendo vindo posteriormente, em 2010, a ratificá-la.

Figura 4 - Cronologia Portugal

Em 2013, o Conceito Estratégico de Defesa Nacional (CEDN) identificou um conjunto de ameaças no ciberespaço e o papel da Defesa na manutenção das infraestruturas críticas, reconhecendo a necessidade de definir uma ENSC e a criação dos organismos técnicos necessários para levantar a capacidade de ciberdefesa nacional (RCM, 2013a), que se vieram a efetivar em 2015 com a criação do Centro de Ciberdefesa (CCD) sob a alçada do Estado-Maior-General das Forças Armadas (EMGFA) e com a aprovação da ENSC.

A ENSC aprovada em 2015 estabeleceu os objetivos e linhas de ação com vista a uma eficaz gestão de crises, uma coordenação da resposta operacional a ciberataques (Figura 5), o desenvolvimento de sinergias nacionais e a intensificação da cooperação nacional, europeia e internacional no domínio do ciberespaço (RCM, 2015). Com o objetivo de garantir um elevado nível de segurança das redes e da informação, Portugal estabeleceu o regime jurídico da segurança do ciberespaço em 2018, através da transposição para o seu quadro legal (Lei n.º 46/2018), da diretiva da UE 2016/1148, de 6 de julho. Posteriormente, em 23 de maio de 2019, foi aprovada a ENSC 2019-2023, que se encontra atualmente em vigor, e reitera a elevada importância do ciberespaço e da capacidade de ciberdefesa para garantir a soberania nacional (RCM, 2019).

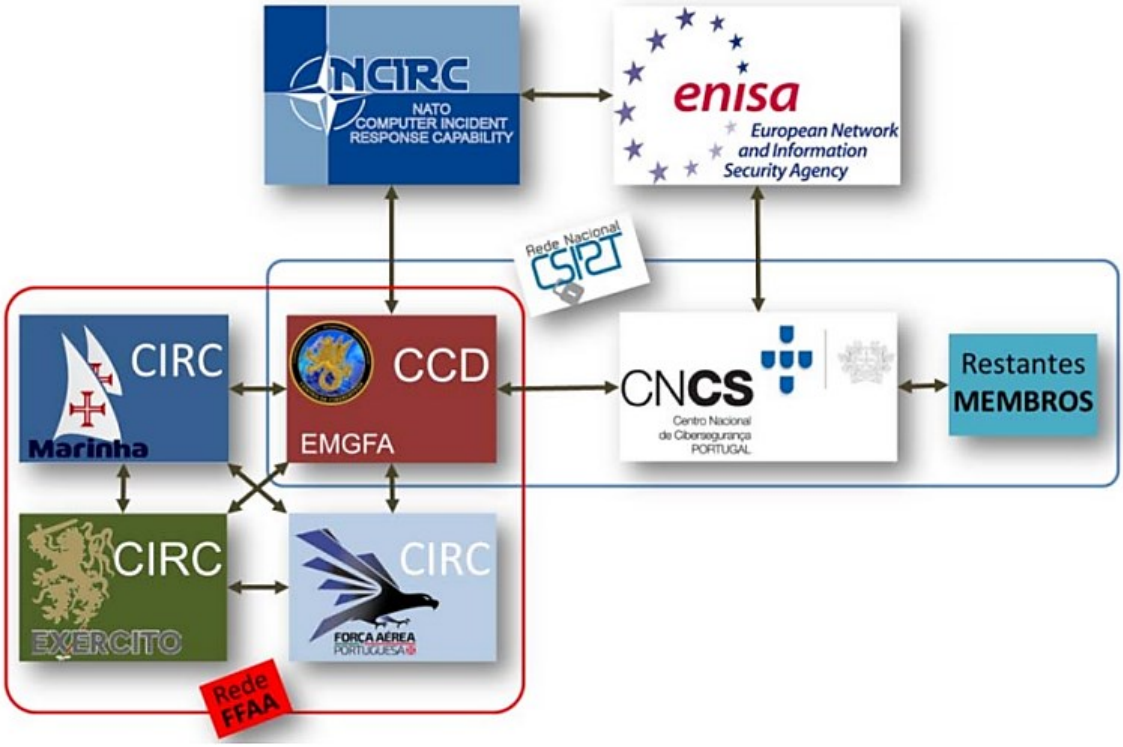

Figura 5 - Coordenação da resposta operacional a ciberataques

Fonte: MDN (2021).

Com vista a cumprir com os objetivos da ENSC 2019-2023, na Lei de Programação Militar (LPM) para o período de 2019-2030, foi triplicada a verba disponível para o investimento na área da ciberdefesa, para um total de 51 milhões de euros (MDN, 2021a).

2.2 Modelo de análise

O modelo de análise visa responder às Questões Derivadas (QD) e QC, de modo a alcançar respetivamente os Objetivos Específicos (OE) e o OG, conforme descrito no Apêndice B.

Face à abrangência do tema, houve a necessidade de o delimitar no domínio temporal, espacial e concetual, conforme preconizado por Santos & Lima (2019, p. 44):

- Temporal, tem como termo de referência de início a RCM n.º 26/2013, de 19 de abril, onde foi definida a orientação estratégica para a ciberdefesa, no quadro da reforma "Defesa 2020", e como termo de referência final, o período da realização deste estudo, julho de 2021.

- Espacial, centrar-se-á nas FFAA Portuguesas e no seu relacionamento com a estrutura nacional de segurança do ciberespaço, com especial enfoque na relação da componente militar (ciberdefesa), com o nível estratégico, e com a componente civil (cibersegurança).

- Concetual, cingir-se-á à realização de entrevistas a especialistas, e à análise da legislação nacional, da OTAN e da UE que contribui para o quadro legal em vigor no domínio do ciberespaço.

2.3 Enquadramento metodológico

Abordou-se a problemática através de uma orientação ontológica construtivista e uma orientação epistemológica interpretativa, fazendo uso de um raciocínio indutivo, e seguindo uma estratégia qualitativa baseada num estudo de caso do objeto da investigação, através de um horizonte temporal transversal (Santos & Lima, 2019).

O desenho de pesquisa é o estudo de caso relativo à necessidade de edificação de um Ramo independente das FFAA, com capacidade de atuar no domínio do ciberespaço, baseando-se na análise documental e recolha de dados das entrevistas.

Para melhor compreensão do objeto de investigação e cumprimento do OG, serão observados fenómenos particulares de modo a estabelecer regras gerais, partindo do particular para o geral, tendo por base uma estratégia qualitativa que incide na análise documental relevante identificada e na análise de entrevistas a especialistas na área da ciberdefesa (Santos & Lima, 2019).

Os instrumentos metodológicos são a análise documental e entrevistas (Santos & Lima, 2019).

A análise documental servirá para efetuar o enquadramento teórico e doutrinário do objeto de estudo, bem como validação do quadro jurídico em vigor e dos compromissos nacionais assumidos com os parceiros estratégicos no domínio do ciberespaço.

As entrevistas aos especialistas na área da ciberdefesa dos Ramos das FFAA, CCD, Centro Nacional de Cibersegurança (CNCS) e do *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) da OTAN, servirão para validação doutrinária, caracterização da capacidade militar atual das FFAA para o domínio do ciberespaço, e identificação de contributos para o modelo de capacitação militar decorrente da edificação de um Ramo independente das FFAA com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações.

Pretende-se ainda responder às questões formuladas, recorrendo à análise documental e às entrevistas semiestruturadas, e efetuar a avaliação e discussão dos resultados, validação dos dados obtidos e apresentação das conclusões, assim como apresentar os contributos para o conhecimento, as limitações e recomendações.

3. Capacidade nacional de ciberdefesa

Neste capítulo pretende-se caracterizar a capacidade nacional de ciberdefesa, com especial enfoque na observação do atual modelo orgânico e funcional das FFAA para atuar no domínio do ciberespaço, e a sua integração com as áreas responsáveis pelos sistemas de informação e comunicações nos diferentes organismos das FFAA, de modo a responder à QD1 e atingir o OE1.

3.1 Estratégia nacional para a segurança do ciberespaço

A ENSC estabelece objetivos e linhas de ação com vista a uma eficaz gestão de crises, uma coordenação da resposta operacional a ciberataques, o desenvolvimento de sinergias nacionais e a intensificação da cooperação nacional, europeia e internacional no ciberespaço (RCM, 2019). Esta estratégia identificou ainda a necessidade de colocar na dependência direta do Primeiro-Ministro a coordenação político-estratégica para a segurança do ciberespaço, conforme Figura 6.

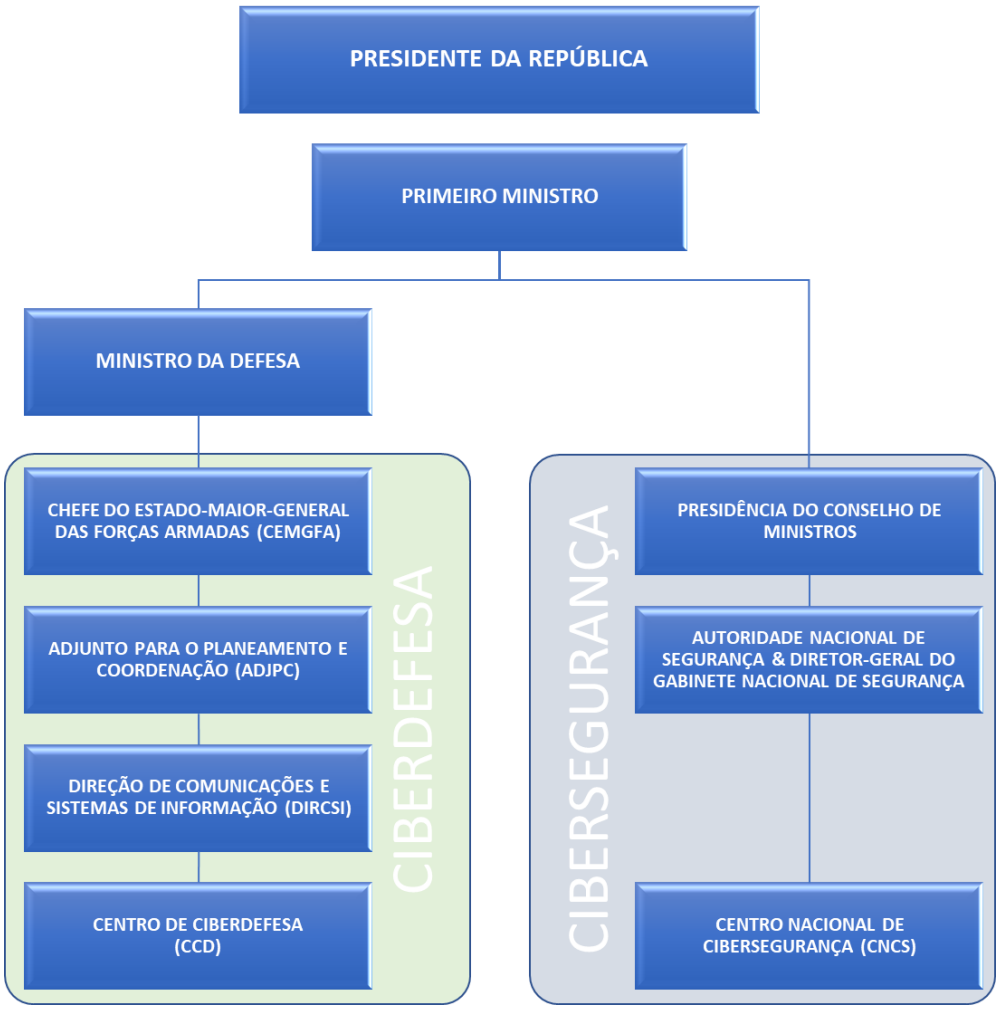

Figura 6 - Estrutura nacional para a segurança do ciberespaço

Fonte: Adaptado de Marques (2018) e Nunes (2020).

Deste modo, o papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas, compete ao CNCS, enquanto a condução de operações militares de modo a assegurar a liberdade de ação do país no ciberespaço, e quando determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional, são da responsabilidade das FFAA, através da capacidade de ciberdefesa (RCM, 2019).

> *As ações e operações militares conduzidas no âmbito da ciberdefesa são executadas no respeito do quadro legal em vigor, obedecendo à mesma lógica e fundamentos que caracterizam a Segurança e a Defesa Nacional.* (MDN, 2013)

3.2 Modelo orgânico das Forças Armadas para atuar no ciberespaço

O atual modelo orgânico das FFAA para atuar no ciberespaço é um modelo distribuído, onde o EMGFA e os Ramos dispõem cada um da sua estrutura de Tecnologias da Informação e Comunicações (TIC) e de cibersegurança/ciberdefesa. Relativamente às TIC, não existe nenhuma relação de interdependência funcional/técnica entre os diversos órgãos das FFAA. Para a ciberdefesa, os Ramos, apesar de disporem de autonomia funcional, encontram-se na dependência técnica do EMGFA, através do Comandante das Operações do CCD (Figura 7), de acordo com a estrutura transitória para a organização de ciberdefesa que se encontra aprovada e implementada (CCD, 2020).

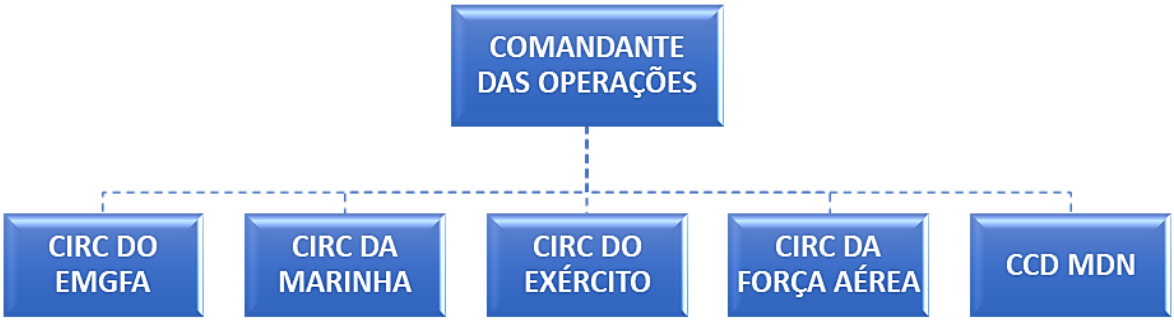

Figura 7 - Comando Técnico dos NCIRC
Fonte: Adaptado de CCD (2020).

3.2.1 Centro de Ciberdefesa

O CCD é um órgão conjunto, inserido na estrutura do EMGFA, conforme Figura 8, constituído por militares dos Ramos das FFAA, com capacidade de atuação no domínio do ciberespaço. (MDN, 2021)

> *Tem como missão garantir a integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação da Defesa Nacional, essenciais ao exercício da nossa soberania, levando a cabo ações de defesa e, eventualmente, a criação de efeitos no, e através do, ciberespaço.* (MDN, 2021)

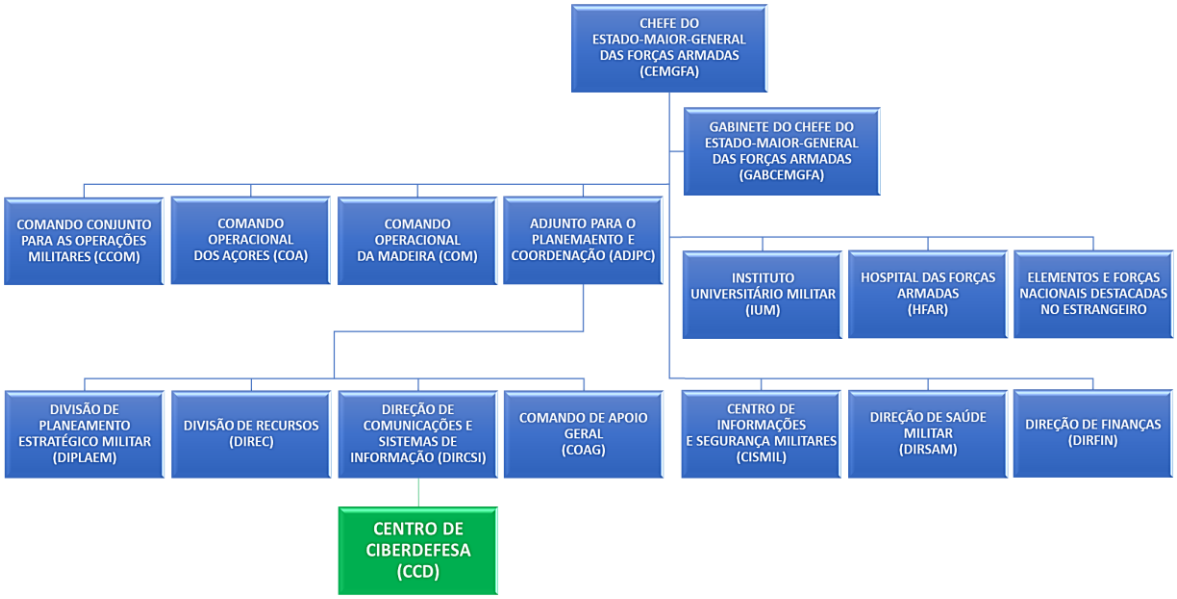

Figura 8 - Estrutura Orgânica do EMGFA

Fonte: Adaptado de SGMDN (s.d.).

Atualmente, o CCD é transitoriamente comandado por um Coronel/Capitão-de-mar-e-guerra, estando previsto o comando ser atribuído a um Brigadeiro-general/Comodoro, e encontra-se dividido em três grandes áreas (Estado-Maior, Operações e Área Tecnológica), conforme Figura 9, e contempla ainda um Centro de Operações (PRTCERTDEF) em regime 24/7 (CCD, 2020). A sua missão e atribuições encontram-se explanadas no Apêndice C.

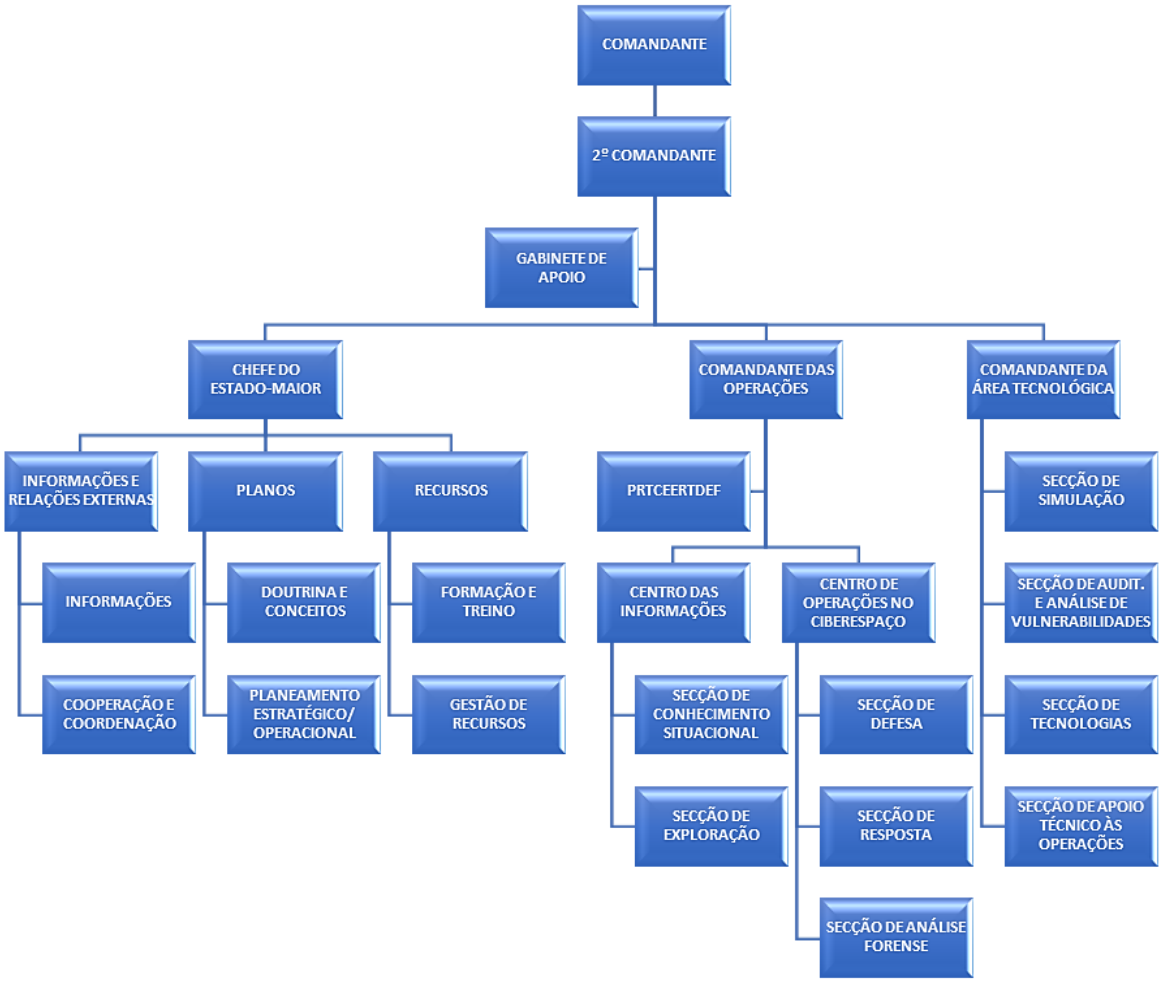

Figura 9 - Organograma do Centro de Ciberdefesa

Fonte: Adaptado de CCD (2020).

> *Na atual Lei Orgânica do EMGFA, o CCD encontra-se debaixo da DIRCSI para operações correntes, no entanto já está contemplada a possibilidade de em operações militares, o comando do CCD ficar debaixo do CCOM [...] A lógica é a DIRCSI criar a capacidade, que posteriormente é utilizada pelo CCOM para operações militares no ciberespaço.* (Marques, 2021)

No decurso da elaboração do Plano de Desenvolvimento da Capacidade de Ciberdefesa (Grupo de Trabalho para o desenvolvimento da Capacidade de Ciberdefesa das Forças Armadas [GT-CCFA], 2019), foi efetuada uma análise de "Forças, Fraquezas, Oportunidades e Ameaças" (SWOT), tendo em vista a caracterização dos ambientes internos e externos, conforme Figura 10.

Figura 10 - Análise SWOT CCD

Fonte: Adaptado de GT-CCFA (2019).

Esta análise identificou, entre outros, o compromisso da estrutura de topo para o desenvolvimento da capacidade, e vontade de integrar a componente de ciberdefesa das FFAA.

3.2.2 Marinha

O modelo orgânico da Marinha para as TIC e para a ciberdefesa contempla uma célula de Ciberdefesa e Tecnologias da Informação e Comunicações, ao nível da Divisão de Operações do Estado-Maior, e na componente técnica, na dependência direta da Superintendência das Tecnologias da Informação, dispõe da Direção de Tecnologias de Informação e Comunicações, onde estão integradas as TIC e o Núcleo de *Computer Incident Response Capability* (NCIRC) da Marinha, conforme Figura 11 (Assunção, 2021).

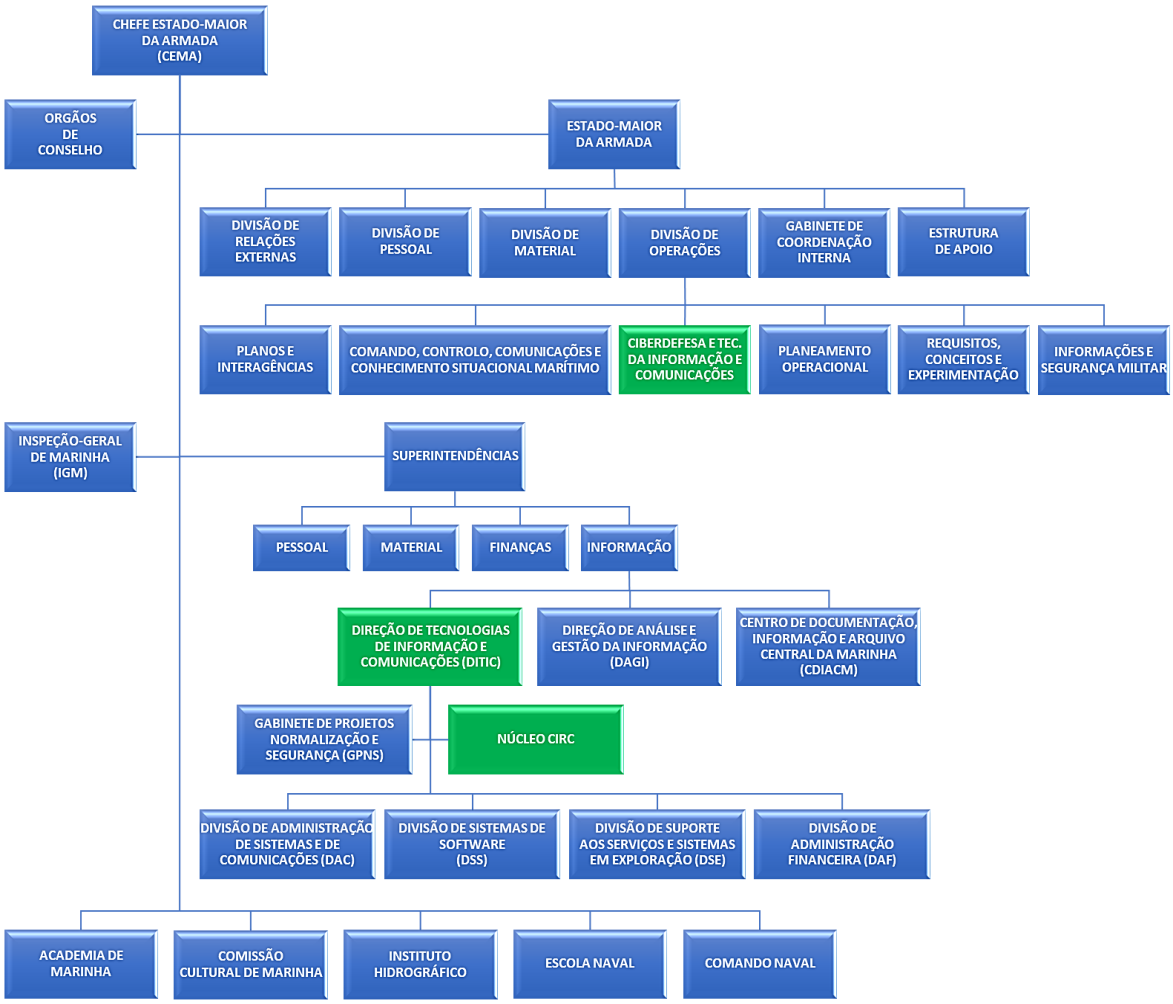

Figura 11 - Estrutura Orgânica da Marinha

Fonte: Adaptado de Secretaria-Geral do Ministério da Defesa Nacional (SGMDN) (s.d.).

3.2.3 Exército

O modelo orgânico do Exército para as TIC e para a ciberdefesa, conforme Figura 12, contempla na direta dependência do Vice-Chefe do Estado-Maior do Exército, uma Direção de Comunicações e Sistemas de Informação (DCSI) que tem sob a sua alçada as TIC e o NCIRC. Ao nível estratégico, no Estado-Maior do Exército, a Divisão de Planeamento de Forças, é a responsável por realizar estudos e elaborar propostas no âmbito do comando e controlo e da ciberdefesa (Exército, s.d.).

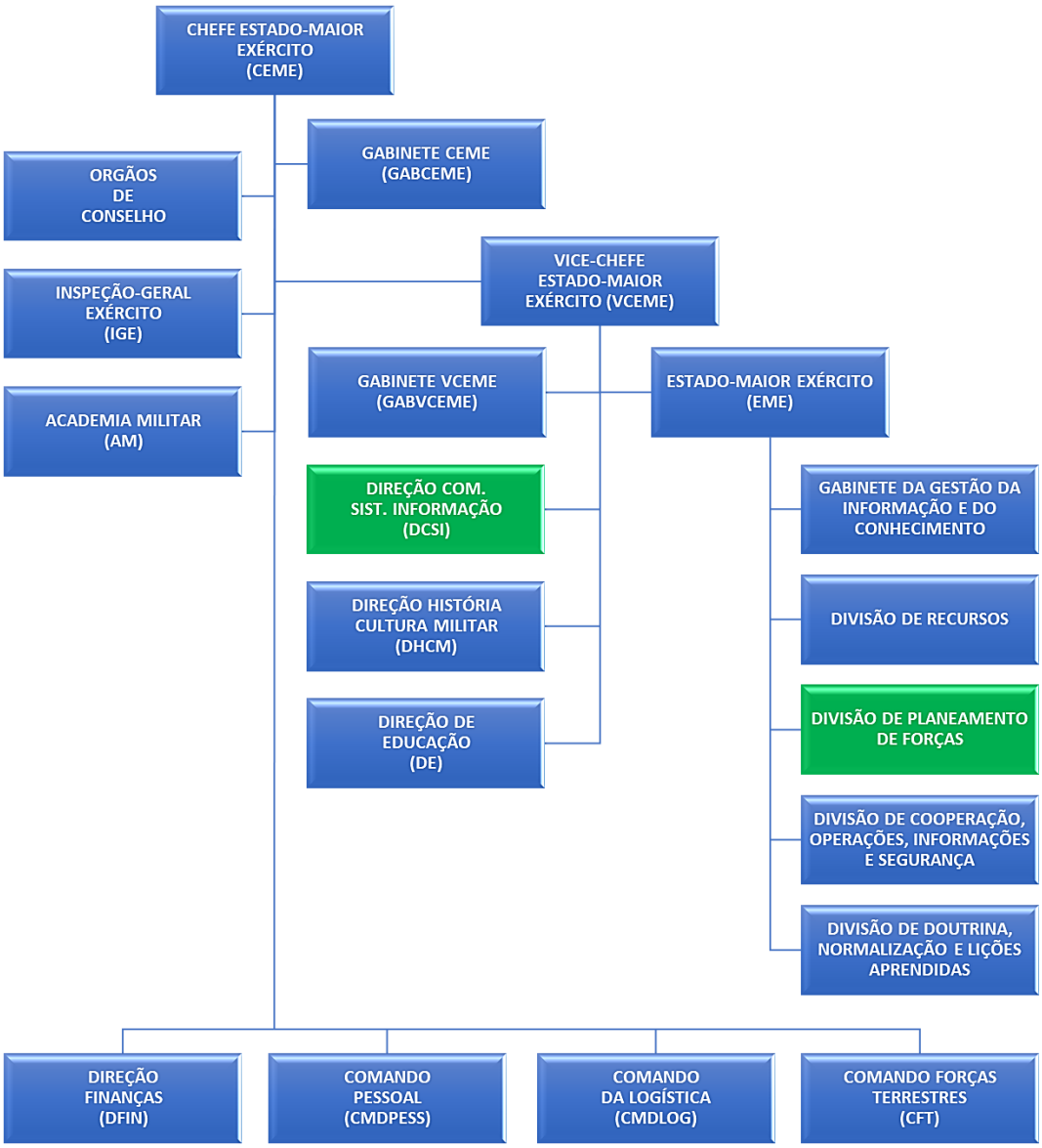

Figura 12 - Estrutura Orgânica do Exército

Fonte: Adaptado de SGMDN (s.d.) e Exército (s.d.).

3.2.4 Força Aérea

O modelo orgânico da Força Aérea (FA) para as TIC e para a ciberdefesa contempla a DCSI na direta dependência do Comando de Logística, que se encontra dividida na componente técnica das Comunicações, Sistemas e Tecnologias, sendo que a última tem na sua dependência direta o NCIRC. Ao nível estratégico, dispõe da Divisão de Comunicações e Sistemas de Informação na direta dependência do Subchefe de Estado-Maior da FA, conforme Figura 13 (Valente, 2021).

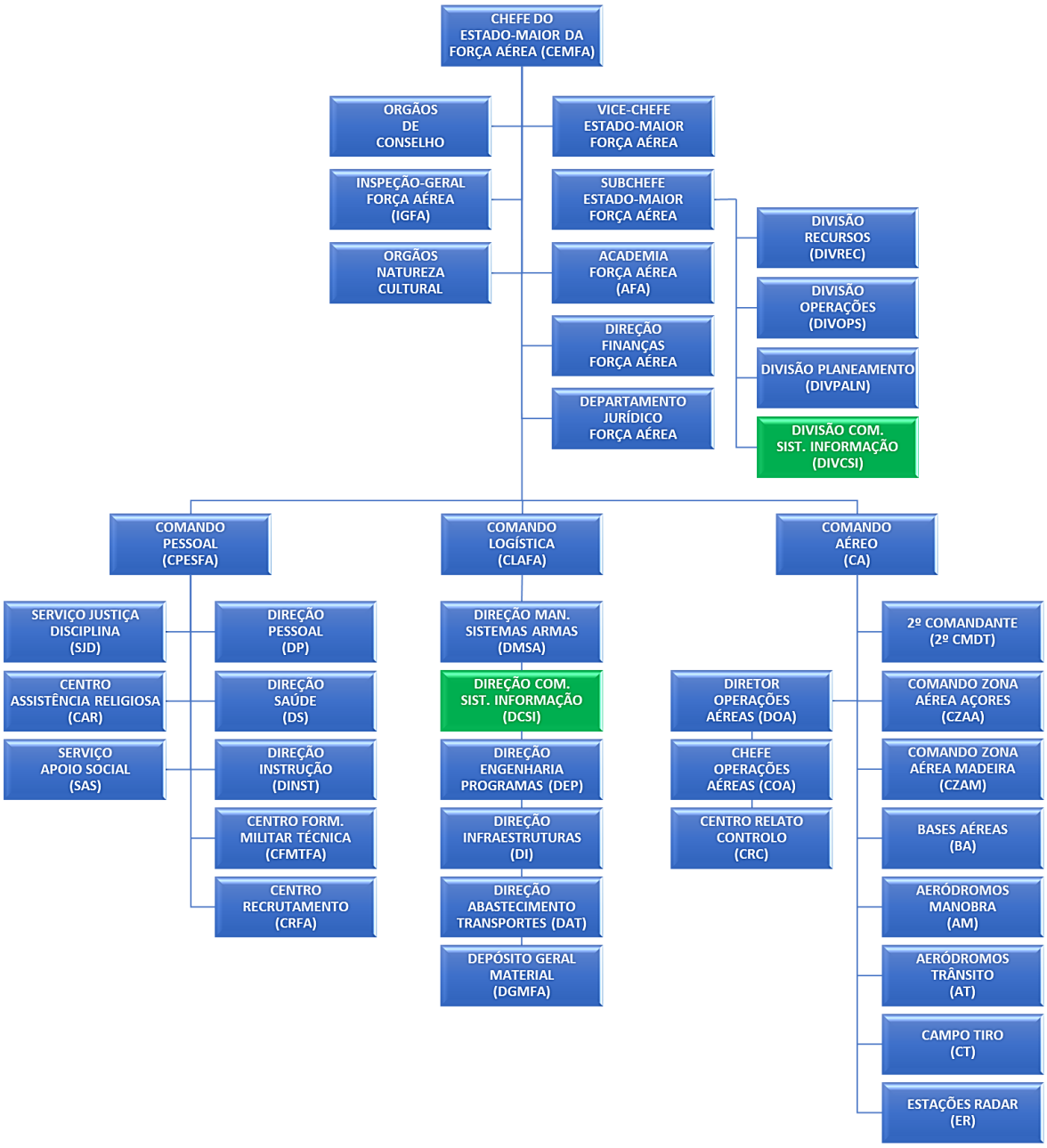

Figura 13 - Estrutura Orgânica da Força Aérea

Fonte: Adaptado de SGMDN (s.d.).

3.3 Análise do modelo orgânico das Forças Armadas para atuar no ciberespaço

A análise do atual modelo orgânico das FFAA para o domínio do ciberespaço, será efetuada com recurso à caracterização dos vetores da metodologia DOTMLPII: Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade.

O atual edifício doutrinário para a ciberdefesa é reduzido e encontra-se na sua maioria desatualizado, sendo a falta de Regras de Empenhamento uma limitação identificada (Assunção, 2021). Atualmente cada Ramo tem a liberdade de emanar doutrina própria, no entanto, encontra-se a ser desenvolvido um esforço por parte do EMGFA para elaboração

de doutrina conjunta que deverá ser materializada no normativo interno do CCD e dos Ramos (Carvalho, 2021; Valente, 2021).

A estrutura descentralizada das TIC torna necessária a existência dos NCIRC dos Ramos para garantir uma melhor interligação da capacidade de ciberdefesa com as TIC (Assunção, 2021). No entanto, o facto do CCD estar enquadrado dentro de uma direção técnica do EMGFA poderá ser um fator de estrangulamento da capacidade de ciberdefesa nacional (Valente, 2021).

Em termos de formação e treino, já existe diversa formação disponível, mas é necessário trabalhar muito esta área, uma vez que a formação consegue elevar o desempenho até um determinado nível, mas o treino também será fundamental para incrementar as competências, caso se pretenda avançar para a produção de armas cibernéticas próprias (Valente, 2021).

Ao nível do material, a grande heterogeneidade de arquiteturas de rede, sistemas e tecnologias nas FFAA, associada à sua estrutura distribuída e à obsolescência dos equipamentos, dificultam uma resposta defensiva e colaborativa dos sistemas das FFAA efetiva e eficaz (Assunção, 2021; Valente, 2021). Atualmente existe um grande investimento nesta área, permitindo a aquisição e manutenção dos equipamentos e infraestruturas tecnológicas necessárias (Carvalho, 2021).

Compete ao CCD, através do Decreto Regulamentar (DR) n.º 13/2015, assumir a direção e coordenação da capacidade nacional de ciberdefesa, no entanto, não existe nenhum normativo que estabeleça uma relação funcional efetiva entre o CCD e os NCIRC dos Ramos (Assunção, 2021). Verifica-se ainda que é necessário envolver ao nível de topo da ciberdefesa, pessoal com visão operacional e capacidade de liderança de equipas, não necessitando de ter elevadas capacidades técnicas na área da ciberdefesa (Carvalho, 2021).

Ao nível do pessoal é onde se encontram os maiores desafios, uma vez que o pessoal disponibilizado pelos Ramos não tem a formação necessária, e o "CCD encontra-se dependente da disponibilidade dos Ramos para recrutar e fornecer recursos humanos para a capacitação da ciberdefesa, sendo que os próprios Ramos não dispõem desses recursos, nem em quantidade, nem com as respetivas competências" (Assunção, 2021; Prates, 2021). No atual modelo, as FFAA não têm atratividade financeira para reter os recursos humanos mais qualificados, e os requisitos de progressão vertical na carreira, em alguns casos, podem tornar-se noutro entrave (Valente, 2021). Por outro lado, com o atual modelo, torna-se

complicado conciliar uma carreira na ciberdefesa com os requisitos de promoção dos Ramos, uma vez que não existe uma especialização nessa área (Carvalho, 2021).

As infraestruturas TIC existentes encontram-se moldadas à realidade de cada Ramo, havendo uma grande heterogeneidade de arquiteturas, sistemas e tecnologias, o que dificulta os esforços de proteção e resposta defensiva e colaborativa dos sistemas das FFAA (Assunção, 2021; Valente, 2021). No entanto, ao nível dos equipamentos de segurança e defesa de perímetro, uma vez que é o CCD que fornece grande parte dos sistemas e equipamentos aos Ramos, acaba por promover uma certa uniformização (Carvalho, 2021).

A constituição dos NCIRC nos Ramos, permite a interoperabilidade entre estes e o CCD, garantindo a coordenação e o trabalho colaborativo e integrado. A interoperabilidade com as entidades externas é efetuada pelo CCD de forma centralizada, de acordo com o DR n.º 13/2015 (Assunção, 2021; Valente, 2021).

3.4 Síntese conclusiva

Neste capítulo caracterizou-se a capacidade nacional de ciberdefesa através da explanação do modelo orgânico de atuação no ciberespaço e a sua integração com as TIC nos diferentes organismos das FFAA.

A análise das entrevistas possibilitou, no subcapítulo 3.3, caracterizar o atual modelo orgânico das FFAA para o domínio do ciberespaço nas dimensões propostas e correspondentes indicadores. Em resposta à QD1, conclui-se que as FFAA têm capacidade para atuar no ciberespaço, no entanto, esta é condicionada pelas fragilidades existentes ao nível doutrinário, organizacional, e sobretudo pela escassez de pessoal.

4. Modelo de edificação da capacidade nacional de operação no ciberespaço

Analisada a atual estrutura nacional de ciberdefesa, importa compreender como esta poderá ser adaptada, de modo ir ao encontro dos objetivos estratégicos de reforço da ciberdefesa, conforme preconizado na Diretiva Estratégica do EMGFA 2021-2023 (2021).

> *A capacitação seria uma mais-valia para a segurança do ciberespaço de interesse nacional, […] quem beneficiaria sobretudo seria Portugal, por dispor de uma capacidade mais robusta e mais credível. Eu acho que está na altura, sinceramente, já temos o CCD desde 2015, vai fazer 6 anos, o CNCS é de 2014, vai fazer 7 anos, e já está na altura de dizer: "E agora, qual é a fase seguinte? Qual é o destino?".* (Marques, 2021)

Com base na perceção obtida através do tratamento dos dados das entrevistas, foram identificados dois modelos orgânicos, mantendo a capacidade de ciberdefesa na dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), uma vez que:

- A maioria dos entrevistados reforçou que as atuais limitações de recursos humanos nas FFAA, em particular na área da ciberdefesa, levam a que a atual capacidade não se encontre completamente consolidada, e segundo Marques (2021), a criação de um Ramo independente para operar no domínio do ciberespaço, com base no panorama atual das FFAA, poderá potenciar uma disrupção demasiado grande.
- O investimento financeiro necessário para a edificação de um novo Ramo, foi apontado como um fator provavelmente incomportável para o país, a curto prazo (Assunção, 2021; Prates, 2021; Valente, 2021).

O primeiro modelo coloca a ciberdefesa sob a alçada do Comando Conjunto para as Operações Militares (CCOM), e as TIC centralizadas, sob a alçada da Direção de Comunicações e Sistemas de Informação (DIRCSI), conforme Figura 14.

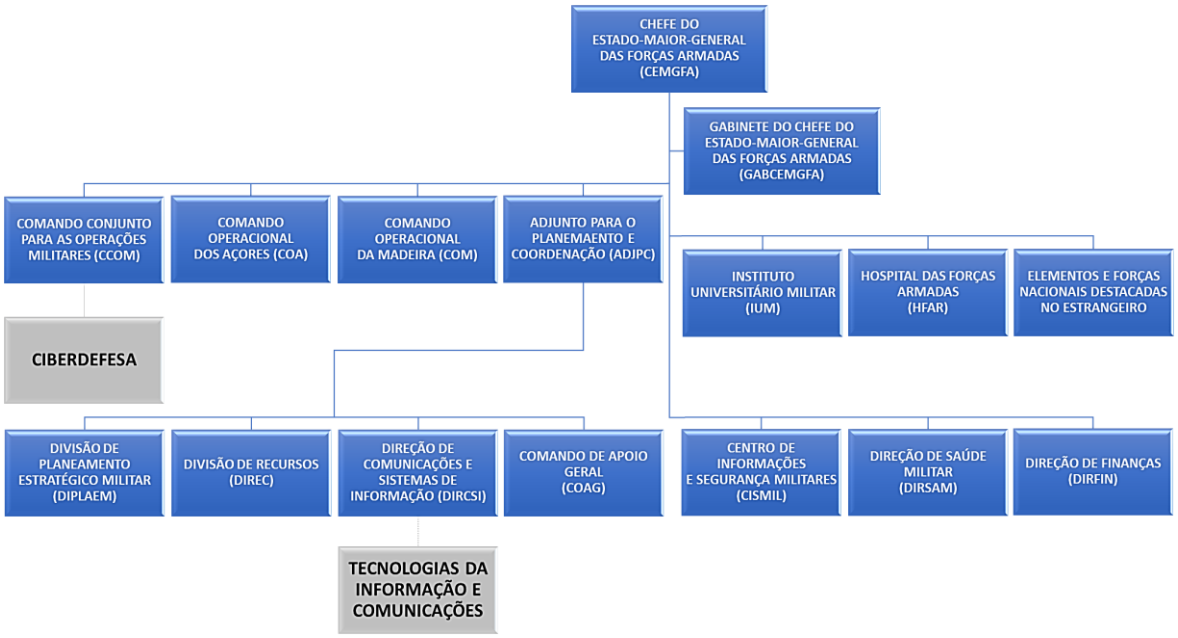

Figura 14 - Estrutura Orgânica para a ciberdefesa (Modelo 1)

Fonte: Adaptado de SGMDN (s.d.).

O segundo modelo (Figura 15), mantém as TIC sob alçada da DIRCSI, no entanto coloca a ciberdefesa como um comando/componente na direta dependência do CEMGFA.

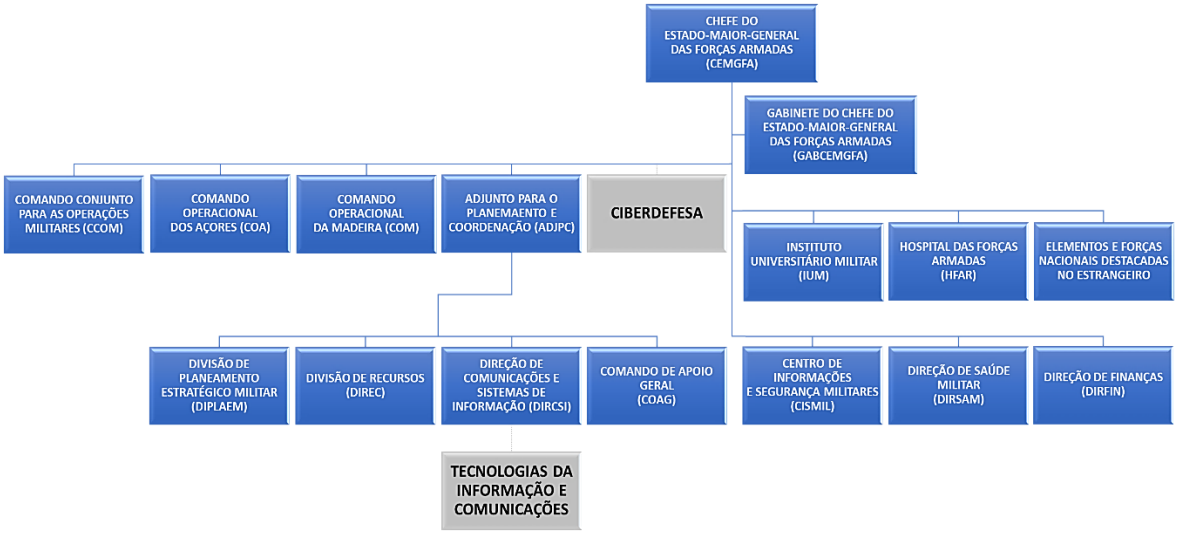

Figura 15 - Estrutura Orgânica para a ciberdefesa (Modelo 2)

Fonte: Adaptado de SGMDN (s.d.).

No subcapítulo 4.1 será proposto o modelo orgânico mais consensual entre os entrevistados. Esse modelo será posteriormente analisado no subcapítulo 4.2, pretendendo-se dar resposta à QD2 para alcançar o OE2, através da elaboração de uma análise SWOT, cuja análise crítica irá contribuir para dar resposta à QC e atingir o OG.

4.1 Modelo orgânico proposto

Com base na informação recolhida nas entrevistas efetuadas, propõe-se como estrutura orgânica para a ciberdefesa o segundo modelo apresentado (Figura 15), mantendo a capacidade de ciberdefesa na direta dependência do CEMGFA.

Não obstante, segundo Marques (2021), as FFAA "devem ter como nível de ambição, reforçar de forma muito significativa a capacidade de ciberdefesa nacional através das FFAA, e devem inclusivamente olhar cada vez mais, e tratar cada vez mais aquela área como uma área de operações militares".

Deste modo, as principais diferenças entre a estrutura orgânica atual (Figura 8), e o modelo proposto (Figura 15), prendem-se nos seguintes pressupostos:

- A ciberdefesa é uma capacidade Operacional, sendo os entrevistados unânimes que deve ser tratada como um verdadeiro domínio de operações militares, e não deverá estar sob uma direção técnica, mas sob um comando operacional, ou mesmo num comando na direta dependência do CEMGFA (Assunção, 2021; Carvalho, 2021; Marques, 2021; Prates, 2021; Valente, 2021).
- A integração de tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações, leva à necessidade da criação/capacitação de uma divisão no EMGFA com valências transversais às necessidades e especificidades de cada Ramo das FFAA, sob a alçada de uma direção técnica, como é o caso da DIRCSI (Assunção, 2021; Carvalho, 2021; Valente, 2021).
- As TIC não deverão estar integradas na estrutura orgânica da ciberdefesa, uma vez que a ciberdefesa é responsável por emanar instruções e recomendações de segurança, assim como é a entidade que tem a competência para efetuar auditorias e inspeções no âmbito das TIC (Carvalho, 2021; Valente, 2021).

Com a edificação desta capacidade no EMGFA, os NCIRC e as TIC existentes nos Ramos deverão progressivamente extinguir-se, na sequência da centralização da capacidade conjunta.

> *No eventual processo de centralização das capacidades e infraestruturas tecnológicas, é fundamental que os recursos humanos existentes nos Ramos integrem a nova capacidade conjunta, permitindo fazer uma transição suave e ao mesmo tempo manter a ligação e conhecimento das especificidades de cada Ramo.* (Assunção, 2021)

4.1.1 Caracterização do modelo

A caracterização do modelo orgânico proposto será efetuada tendo por base a análise dos vetores DOTMLPII, fundamentada nas entrevistas efetuadas aos especialistas.

A alteração da atual estrutura distribuída para uma estrutura centralizada de ciberdefesa e TIC sob a alçada do CEMGFA, terá como principal vantagem uma organização mais simples, garantindo uma doutrina única e transversal às FFAA (Assunção, 2021).

Ao nível da formação e treino, poderiam ser centralizadas as escolas de formação, na área da cibersegurança/ciberdefesa e TIC, sendo para tal necessário um esforço de homogeneização dos sistemas, infraestruturas e tecnologias. Desta forma, será expectável uma redução de pessoal que é necessário treinar e formar (Prates, 2021; Valente, 2021). Por outro lado, a ciberdefesa deixa de ficar dependente da disponibilidade dos Ramos para poder enviar o pessoal que se encontra nos NCIRC dos Ramos às ações de treino (Carvalho, 2021).

Outra grande vantagem identificada é a economia de escala ao nível da aquisição de material e licenciamento, o que irá contribuir para a interoperabilidade dos sistemas (Carvalho, 2021).

No pessoal, é onde se observa maior vantagem, dado que o recrutamento e retenção são fatores críticos, e a centralização poderá possibilitar a redução das necessidades de pessoal. Nesta perspetiva, poderá ser necessário repensar o modelo de recrutamento e seleção para torná-lo mais apelativo, bem como uma eventual adaptação das carreiras para a área do saber das comunicações e sistemas de informação, que permitam menor rotatividade nos cargos técnicos (Assunção, 2021; Prates, 2021; Valente, 2021).

Apesar da centralização permitir uma organização mais simples e uma liderança "a uma voz" mais robusta e mais eficaz, os Ramos poderão eventualmente perder alguma capacidade de decisão sobre os processos relacionados com as TIC, uma vez que deixam de ter a capacidade e os recursos próximos de si (Valente, 2021).

Ao nível das infraestruturas tecnológicas "deve-se caminhar para a sua homogeneização, o que irá facilitar a interoperabilidade, não só nas tarefas de administração, gestão e defesa da rede, mas também irá permitir incrementar o treino do pessoal, criar políticas/configurações de segurança e gerar modelos de deteção de ameaças muito mais ricos, contribuindo para aumentar a robustez e resiliência das redes das FFAA contra ciberataques." (Assunção, 2021). Ao nível das infraestruturas, será necessário algum espaço adicional para suportar o eventual incremento de pessoal, no entanto, existem instalações

que poderão ser utilizadas, necessitando apenas de ser preparadas para albergar a capacidade (Carvalho, 2021).

A interoperabilidade não deverá ser um fator com impacto relevante, uma vez que com a centralização da capacidade de ciberdefesa e TIC no EMGFA, passará a estar garantida a interoperabilidade interna nas FFAA, permanecendo a interoperabilidade com entidades externas garantida através do EMGFA, tal como já existe, e que previsivelmente passará a ter maior relevância (Carvalho, 2021; Valente, 2021).

4.2 Análise do modelo orgânico proposto

Para analisar o modelo orgânico proposto no subcapítulo 4.1, será empregue uma análise SWOT, que será representada na Figura 16, identificando as forças, fraquezas, oportunidades e ameaças decorrentes do modelo proposto, visando responder à QD2 e alcançar o OE2.

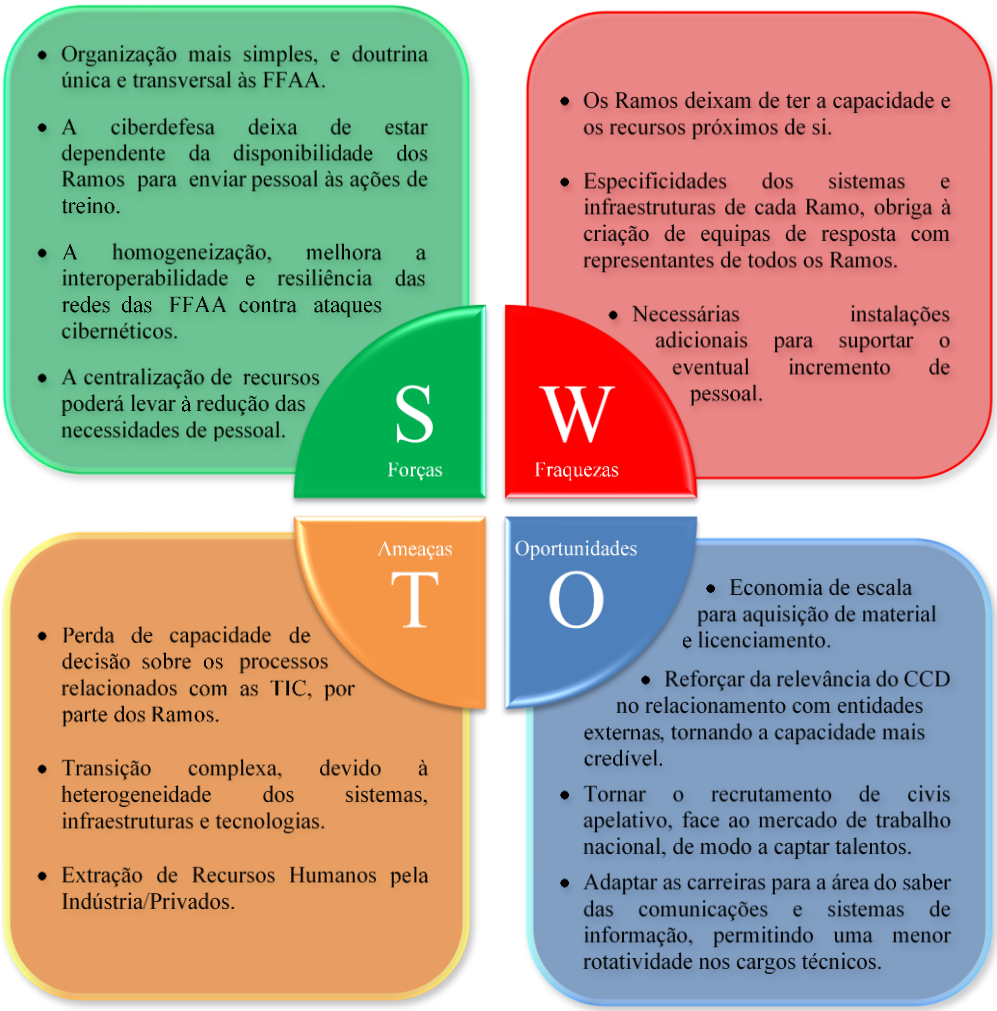

Figura 16 - Análise SWOT ao modelo orgânico proposto

Decorrente das entrevistas e da análise efetuada (Figura 16), considera-se que o modelo proposto no subcapítulo 4.1, apresenta potencialidades que contribuem para uma edificação gradual e consistente da ciberdefesa, permitindo a longo prazo, eventualmente alcançar um Ramo independente para atuar no domínio do ciberespaço. Numa perspetiva de racionalização de recursos, economia de escala e uniformização da infraestrutura, recomenda-se que as TIC das FFAA sejam centralizadas no EMGFA.

4.3 Síntese conclusiva

Neste capítulo foi proposto e analisado um modelo orgânico com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações.

Como resposta à QD2, foi desenvolvida, no subcapítulo 4.2, a matriz SWOT ilustrada na Figura 16, onde são identificadas as forças, fraquezas, oportunidades e ameaças decorrentes do modelo proposto, sendo de evidenciar as vantagens ao nível dos recursos humanos e homogeneização da infraestrutura.

Em resposta à QC, conclui-se que, a curto prazo não é adequado edificar um Ramo independente das FFAA com capacidade para atuar no domínio do ciberespaço, mas deverão ser dados passos nesse sentido, através de uma estratégia genética de capacitação da ciberdefesa. Recomenda-se a centralização de recursos na área da ciberdefesa e das TIC no EMGFA, através da implementação do modelo proposto, como um estágio intermédio de capacitação da ciberdefesa, numa perspetiva de racionalização de recursos, economia de escala e uniformização da infraestrutura das FFAA, devendo ser edificada com recurso a militares e civis, para ultrapassar os atuais constrangimentos de pessoal.

5. Conclusões

Os desafios atuais da cibersegurança representam o início de uma era tecnológica, em que os ciberataques estimulam que adversários potencialmente mais fracos possam superar um poder militar convencional superior de forma instantânea e difícil de rastrear, colocando em risco a soberania da nação. Com a emergente relevância do ciberespaço, e elevada importância que a OTAN e a UE admitem que este possa vir a ter, Portugal como membro destas organizações, deverá promover a edificação de uma capacidade de ciberdefesa robusta e capaz de fazer face aos desafios no domínio do ciberespaço.

Neste âmbito, o presente TII teve como propósito avaliar a adequabilidade de edificação de um Ramo independente das FFAA, com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações. Encontrando-se delimitado nos domínios: temporal, ao período de abril de 2013 a julho de 2021; espacial, às FFAA portuguesas e ao seu relacionamento com a estrutura nacional de segurança do ciberespaço; e concetual, à análise documental, e entrevistas a especialistas.

Assumiu-se nesta investigação uma orientação ontológica construtivista e uma orientação epistemológica interpretativa, fazendo uso de um raciocínio indutivo, através de uma estratégia qualitativa baseada num estudo de caso do objeto da investigação, visando dar resposta à QC da investigação: "*Será adequado edificar um Ramo independente das FFAA com capacidade para aturar no domínio do ciberespaço?*"

A estrutura do TII é composta por cinco capítulos: introdução; enquadramento; capacidade nacional de ciberdefesa; modelo de edificação da capacidade nacional de operação no ciberespaço; e conclusões.

Relativamente aos objetivos desta investigação, a caracterização da capacidade nacional de ciberdefesa através da explanação do modelo orgânico de atuação no ciberespaço e a sua integração com as TIC nos diferentes organismos das FFAA, permitiu caracterizar o atual modelo orgânico das FFAA para o domínio do ciberespaço nas dimensões propostas e correspondentes indicadores, possibilitando responder à QD1, atingindo-se o OE1.

Seguidamente, com base na bibliografia analisada e na perceção obtida através do tratamento dos dados das entrevistas, foi proposto e analisado um modelo orgânico com capacidade de atuar no ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações. Sustentada na caracterização dos vetores

DOTMLPII, foi elaborada uma matriz SWOT para o modelo proposto, permitindo alcançar as dimensões propostas e correspondentes indicadores, respondendo à QD2 e alcançando o OE2. A análise crítica da matriz SWOT permitiu ainda dar resposta à QC, alcançando-se o OG da investigação (*Avaliar a adequabilidade de edificação de um Ramo independente das FFAA, com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações*).

Deste modo, recomenda-se a centralização de recursos na área da ciberdefesa e das TIC no EMGFA, numa perspetiva de racionalização de recursos, economia de escala e uniformização da infraestrutura das FFAA, uma vez que, considera-se que a curto prazo não é adequado edificar um Ramo independente das FFAA com capacidade para atuar no domínio do ciberespaço, embora devam ser dados passos nessa direção, de modo que eventualmente possa ser alcançado a médio/longo prazo, sendo para tal recomendável a implementação do modelo proposto, como um estágio intermédio para a capacitação da ciberdefesa nacional.

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

Neste âmbito, os resultados deste estudo constituem um significativo contributo para a edificação da capacidade de ciberdefesa e segurança do ciberespaço de interesse nacional, permitindo beneficiar de uma capacidade de ciberdefesa mais robusta e mais credível. Identifica-se como principal **contributo para o conhecimento** a proposta dum modelo centralizado de edificação da capacidade de ciberdefesa nacional e integração de tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações.

Durante a realização do trabalho foram identificadas duas principais **limitações da investigação**. Primeiramente elenca-se o facto do percurso metodológico ter sido sustentado na bibliografia analisada e no entendimento dos especialistas entrevistados, sendo que este último encontra-se sujeito a enviesamentos baseados na perceção individual. E a segunda limitação prende-se pelo facto de não ter havido oportunidade de entrevistar o especialista na área da ciberdefesa do Exército, como inicialmente proposto.

No que concerne a **estudos futuros**, afigura-se interessante aprofundar o estudo, com vista à operacionalização do modelo proposto através de um grupo de trabalho constituído por representantes do EMGFA, dos Ramos, e de outros organismos considerados relevantes, para validar a sua exequibilidade e aceitabilidade.

A principal **recomendação de ordem prática** que decorre deste trabalho, prende-se com a necessidade de edificar, operacionalizar e consolidar, com a maior brevidade possível, uma capacidade de ciberdefesa robusta, com vista a assegurar a condução de operações militares no ciberespaço, garantindo a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a sua exploração proativa para impedir ou dificultar o uso hostil contra o interesse nacional, conforme preconizado na RCM n.º 92/2019, de 05 de junho.

Referências bibliográficas

CCD. (2020). *Regulamento Interno do Centro de Ciberdefesa das Forças Armadas*. Lisboa: Centro de Ciberdefesa.

Conceito.de. (2011a). Conceito de eficácia [Página *online*]. Retirado em 16 de junho de 2021, de https://conceito.de/eficacia

Conceito.de. (2011b). Conceito de eficiência [Página *online*]. Retirado em 16 de junho de 2021, de https://conceito.de/eficiencia

Corporate Finance Institute. (2021, 16 de junho). Economies of Scale - Definition, Types, Effects of Economies of Scale [Página *online*]. Retirado de https://corporatefinanceinstitute.com/resources/knowledge/economics/economies-of-scale/

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

CUE. (2018). *EU Cyber Defence Policy Framework (2018 update).* Bruxelas: Council of the European Union.

DOD. (2021). *DOD Dictionary of Military and Associated Terms*. Washington DC: The Joint Staff.

Ebbesson, B., & Olsson, T. (2008). *Managing divergences in IT infrastructure standardization* (Master thesis in IT Management). Chalmers University of Technology and University of Gothenburg, Göteborg - Sweden.

EC. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruxelas: European Commission.

EC. (2020a). *The EU's Cybersecurity Strategy for the Digital Decade*. Bruxelas: European Commision.

EC. (2020b, 16 de dezembro). The Cybersecurity Strategy [Página *online*]. Retirado em 02 de abril de 2021, de https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy

EMA. (2006). *PDA2 - Glossário de Sistemas e Tecnologias de Informação e Comunicação (GlosSTIC).* Lisboa: Estado-Maior da Armada.

EMGFA. (2021). *Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2021-2023*. Lisboa: Chefe do Estado-Maior-General das Forças Armadas.

Exército. (s.d.). Cadeia de Comando do Exército [Página *online*]. Retirado de https://www.exercito.pt/pt/quem-somos/organizacao

Forsling, C. (2016, 28 de junho). Should Cyber Warfare Have Its Own Branch? [Página *online*]. Retirado em 11 de março de 2021, de https://taskandpurpose.com/community/cyber-warfare-branch/

GT-CCFA. (2019). *Plano de Desenvolvimento da Capacidade de Ciberdefesa.* Lisboa: Estado-Maior-General das Forças Armadas.

Klimburg, A. (2012). *National cyber security framework manual.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Lei n.º 46/2018, de 13 de agosto (2018). *Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.* Diário da República, 1.ª Série, 155. 4031 a 4037. Lisboa: Assembleia da República.

Lei Orgânica n.º 6/2014, de 01 de setembro (2014). *Procede à primeira alteração à Lei Orgânica de Bases da Organização das Forças Armadas, aprovada pela Lei Orgânica n.º 1-A/2009, de 7 de julho*. Diário da República, 1.ª Série, 167. 4597 a 4611. Lisboa: Assembleia da República.

Lynn III, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs, 89*(5), 97-108. Retirado de http://www.jstor.org/stable/20788647

Marques, A. G. (2018, novembro). Estratégia Nacional de Segurança do Ciberespaço 2.0 - Governação e execução. Em: Centro Nacional de Cibersegurança. Lisboa.

Marrone, A., & Sabatino, E. (2021, fevereiro). *Cyber Defence in NATO Countries: Comparing Models.* Paper apresentado no Istituto Affari Internazionali, Roma. Retirado em 01 de abril de 2021, de https://www.iai.it/sites/default/files/iaip2105.pdf

MDN. (2013). *Orientação para a política de Ciberdefesa* (Despacho n.º 13692/2013, de 28 de outubro). Lisboa: Ministro da Defesa Nacional.

MDN. (2014). *Diretiva Ministerial de Planeamento de Defesa Militar* (Despacho n.º 11400/2014, de 11 de setembro). Lisboa: Ministro da Defesa Nacional.

MDN. (2021). O Centro de Ciberdefesa [Página *online*]. Retirado em 02 de abril de 2021, de https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx

MDN. (2021a). *Enquadramento da Ciberdefesa*. Retirado em 02 de abril de 2021, de https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/enquadramento/

Neves, P. J. (2015). *Resposta a incidentes de segurança da informação: uma abordagem DOTMLPI-I* (Dissertação para a obtenção do Grau de Mestre em Segurança da Informação e Direito no Ciberespaço). Escola Naval, Almada.

Nunes, P. F. (2020). *A edificação da capacidade de ciberdefesa nacional* (Trabalho de Investigação Individual). Instituto Universitário Militar, Lisboa.

OTAN. (2014, 05 de setembro). Wales Summit Declaration [Página *online*]. Retirado em 23 de junho de 2021, de https://www.nato.int/cps/en/natohq/official_texts_112964.htm

OTAN. (2015). *Informal Interorganizational Military Glossary of Abbreviations, Terms and Definitions Related to Conflict Prevention (CP) and Defence and Related Security Capacity Building (DCB).* Retirado em 15 de junho de 2021, de https://www.cimic-coe.org/resources/external-publications/nato-eu-un-glossary-on-dcb-and-cp.pdf

OTAN. (2020a). *Allied Joint Doctrine for Cyberspace Operations (AJP-3.20)* (Edition A Version 1 ed.). Reino Unido: NATO Standardization Office (NSO).

OTAN. (2020b). Cyber Defence [Página *online*]. Retirado em 11 de março de 2021, de https://www.nato.int/cps/en/natohq/topics_78170.htm

PE. (2016). *Concerning measures for a high common level of security of network and information systems across the Union* (Directive (EU) 2016/1148 of the European Parliament and of the Council). *Official Journal of the European Union,* L(194), pp. 1-30. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

PE. (2019). *On ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU)* (Regulation (EU) 2019/881, de 17 de abril). *Official Journal of the European Union*, L(151), pp. 15-69. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

RCM n.º 19/2013, de 05 de abril (2013a). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1ª Série, 67, 1981-1995. Lisboa: Presidência do Conselho de Ministros.

RCM n.º 26/2013, de 19 de abril (2013b). *Aprova as linhas de orientação para a execução da reforma estrutural da defesa nacional e das Forças Armadas, designada por Reforma «Defesa 2020»*. Diário da República, 1ª Série, 77, 2285-2289. Lisboa: Presidência do Conselho de Ministros.

RCM n.º 36/2015, de 12 de junho (2015). *Aprova a Estratégia Nacional de Segurança do Ciberespaço* (Revogado pela RCM n.º 92/2019, de 05 de junho de 2019). Diário da República, 1ª Série, 113, 3738-3742. Lisboa: Presidência do Conselho de Ministros.

RCM 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.

Ribeiro, A. S. (2009). *Teoria geral da estratégia*. Coimbra: Almedina.

Santos, L. A., & Lima, J. M. (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação* (2.ª edição, revista e atualizada). Pedrouços: Instituto Universitário Militar. Retirado em 06 de junho de 2021, de https://sites.ium.pt/moodle/course/view.php?id=186

SGMDN. (s.d.). Forças Armadas [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/defesa/organizacao/forcasarmadas/

USCYBERCOM. (2018). *Joint Publication 3-12: Cyberspace Operations* (Revision of Joint Publication 3-12 dated 05 February 2013). Maryland: Joint Chiefs of Staff.

Apêndice A - Corpo de conceitos

Aceitabilidade – "está estruturada sobre três requisitos fundamentais e igualmente relevantes: a consistência entre os objectivos fixados pelo Governo, em função das expectativas dos públicos de interesse, e os resultados da modalidade de acção, avaliada pela análise da reacção dos públicos de interesse; a atractividade desses resultados, em termos de benefícios, de local e de tempo de materialização previstos e aceites pelo Governo e pelos cidadãos, avaliada pela análise do retorno; o tipo e a importância dos riscos decorrentes da materialização da modalidade de acção, avaliada pela análise do risco. […] está centrada na observância do princípio da liberdade de acção, isto é, em assegurar o controlo dos factores que apoiam a acção própria e dificultam a do contrário no espaço e no tempo. Como tal, uma modalidade de acção aceitável, deve: adquirir, manter e explorar a iniciativa pelo maior tempo e área possível (iniciativa); minimizar a vulnerabilidade dos planos, das acções, das relações e dos sistemas estratégicos próprios à manipulação e interferência dos contrários (segurança); explorar as condições do meio para viabilizar a melhor materialização do objectivo prioritário fixado (ponto conveniente); garantir o momento, a duração e o ritmo da acção que assegurem a melhor materialização do objectivo prioritário fixado (administração do tempo)" (Ribeiro, 2009, p. 194).

Adequabilidade – "está associada, quer à lógica em que se baseia e à forma como cria e/ou mantém a vantagem estratégica, quer, […] à medida em que considera os desafios do ambiente externo (problemas e eventualidades); se fundamenta ou desenvolve os recursos e as capacidades nacionais, edificando ou explorando as sinergias internas e com aliados (potencialidades) e colmatando as deficiências do potencial nacional (vulnerabilidades); é consistente com a cultura nacional e o contexto político. Em suma, a adequabilidade é o critério que avalia se a modalidade de acção contempla as circunstâncias em que o Estado actua e tem possibilidade de desenvolvimento. […] é muito comum enfatizar a importância da harmonia entre os ambientes externo e interno. Contudo, o ponto mais importante dessas avaliações, é a identificação se a estratégia faz sentido face ao objectivo a materializar, e se, nessa óptica, apresenta deficiências que necessitem de ser colmatadas, o que estabelece a ligação para a avaliação da exequibilidade" (Ribeiro, 2009, p. 190).

Capacidade militar – "o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade" (MDN, 2014).

Cibercrime – "entendem-se os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa" (RCM, 2019).

Ciberdefesa – "consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço" (RCM, 2019).

Ciberespaço – "consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação" (RCM, 2019).

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, 2019).

Comando – unidade, organização, ou área, sob o comando de um militar, ao qual é conferira a autoridade para a direção, coordenação e controlo das forças sob o seu comando (OTAN, 2015).

Componente – estrutura de comando com capacidades específicas, responsável pelo planeamento operacional e condução de operações subordinadas através de um comando superior, ou como parte de uma força conjunta (OTAN, 2015). Segundo a Lei Orgânica n.º 6/2014, de 01 de setembro, os comandos de componente são colocados na dependência direta do CEMGFA, "de acordo com as modalidades de comando e controlo aplicáveis a situações específicas de emprego operacional de forças e meios, a definir caso a caso".

Doutrina – "numa perspetiva militar, a Doutrina aparece ligada ao modo como são conduzidas as operações de combate, sejam as manobras ou as campanhas, ou seja, os princípios fundamentais que permitem a

utilização coordenada de uma ou mais forças militares para atingir um objetivo comum. A Doutrina baseia-se nos princípios comuns construídos sobre as lições aprendidas durante as operações militares, através de treinos e exercícios" (Neves, 2015, p. 51).

Economia de escala – é a vantagem obtida, em termos de preço-por-unidade produzida/adquirida, devido ao incremento da produção, ou à aquisição de produtos em grandes quantidades (Corporate Finance Institute, 2021).

Eficácia – "é a capacidade de alcançar o efeito esperado ou desejado através da realização de uma ação […] independente de tempo e de recursos utilizados" (Conceito.de, 2011a).

Eficiência – "é o uso racional dos meios dos quais se dispõe para alcançar um objetivo previamente determinado. Trata-se da capacidade de alcançar os objetivos e as metas programadas com o mínimo de recursos disponíveis e tempo, conseguindo desta forma a sua optimização" (Conceito.de, 2011b).

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, cit. por Nunes, 2020, p. Apd A-2).

Exequibilidade – "está associada à avaliação dos recursos e capacidades estratégicas necessárias à operacionalização da modalidade de acção, e à identificação das deficiências que necessitam de ser colmatadas, bem como da possibilidade de o fazer, de forma a garantir o sucesso. […] depende da disponibilidade de meios humanos e materiais para empreender e sustentar as acções que permitam alcançar ou preservar os objectivos. […] Para isso, numa modalidade de acção exequível os meios devem: ter o seu emprego coordenado e direccionado para cada objectivo (coordenação); ser concentrados, com superioridade, no local e tempo que permitam a melhor materialização do objectivo prioritário fixado (concentração), ser orquestrados para que a sua aplicação no local e no tempo, garanta a melhor materialização do objectivo prioritário fixado (orquestração)" (Ribeiro, 2009, p. 192).

Infraestruturas – "tudo o que se refere com a disponibilização de instalações adequadas à preparação e condução das operações. Também aqui é importante garantir que as Infraestruturas existentes permitem responder de forma satisfatória aos requisitos de manutenção em tempo de paz e aos requisitos operacionais em tempo de crise. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, oficinas, armazéns, centros de dados, estradas, distribuição de energia elétrica e água, entre outras" (Neves, 2015, p. 53).

Interoperabilidade – coloca "em destaque a importância de existir uma abordagem comum entre as várias entidades ou equipas que participam nas operações. O estabelecimento desta abordagem comum implica que se utilize um conjunto de conceitos partilhados entre as partes, que todos entendam como válidos. Isto pode ser conseguido através de políticas que definam procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo […] por isso a Interoperabilidade assume um papel de destaque na edificação de uma capacidade operacional" (Neves, 2015, p. 53).

Liderança – "surge diretamente ligada à Formação, preocupando-se essencialmente com a preparação das chefias para uma abordagem profissional da operação, ou seja ao desenvolvimento da competência profissional para comandar. É fundamental que o líder seja capaz de compreender o objetivo que lhe é apresentado e que conduza a ação para que este seja alcançado com sucesso. Tem de ter a capacidade de dirigir e motivar os membros da equipa, com profissionalismo, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão" (Neves, 2015, p. 52).

Material – "refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais. Esta dimensão abrange desde os equipamentos, à tecnologia, às armas, ou as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão. Os problemas que surgem nesta área podem ter soluções de natureza material, adquirindo o artigo necessário para a sua resolução. Por outro lado, também podem ser problemas que não sejam resolúveis através de qualquer aquisição, ou seja, terão de ter uma solução não-material, implicando assim soluções que envolvam alterações nas outras dimensões, como por exemplo na doutrina, na organização ou no treino" (Neves, 2015, p. 52).

Operações defensivas no ciberespaço – ações defensivas no, e através do, ciberespaço, para preservar a liberdade de ação das forças amigas no ciberespaço (OTAN, 2020a, pp. LEX-2).

Operações no ciberespaço – consistem no conjunto de ações desenvolvidas no, e através do, ciberespaço, com o propósito de preservar a liberdade de ação das forças amigas e/ou criar efeitos no ciberespaço para alcançar os objetivos definidos pelo comandante" (OTAN, 2020a, pp. LEX-2).

Operações ofensivas no ciberespaço – ações desenvolvidas no, e através do, ciberespaço, que projetem poder para criar efeitos, com vista a alcançar objetivos militares (OTAN, 2020a, pp. LEX-3).

Organização – "diz respeito ao modo como os indivíduos se constituem como equipas, e estas em unidades operacionais, executando as funções que lhes são determinadas, de forma a contribuírem para o sucesso da missão. Estas unidades operacionais são suportadas numa estrutura que permite que funcionem de forma coordenada" (Neves, 2015, p. 51).

Pessoal – "o mais importante é garantir que este possui as qualificações necessárias para o desempenho da missão, quer considerando as necessidades em tempo de paz, quer em tempo de crise. O fator humano e a componente social são determinantes, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e disponibilizarem-lhes a formação adequada. Por outro lado, é preciso considerar que para algumas missões, o pessoal pode não ter as competências necessárias, sendo por isso necessário envolver pessoal externo ou parceiros civis, como sejam as empresas do setor tecnológico ou outras, para que se possa cumprir a missão. Quando identificadas lacunas na formação do nosso pessoal, ou o surgimento da necessidade de novas competências relevantes para a missão, deve ser feita a ponderação de alteração do plano de formação previsto para os diferentes papéis que os elementos desempenham no seio da equipa ou a contratualização do serviço a entidades externas. Finalmente há que considerar um quadro de pessoal que garanta a disponibilidade dos recursos humanos necessários quer em tempo de paz quer em tempo de crise" (Neves, 2015, p. 53).

Racionalização de recursos – tem por base a otimização das capacidades atualmente existentes, "de acordo com o princípio orientador da concentração, sem prejuízo do equilíbrio necessário ao cumprimento de missões em todo o território nacional, visando a economia de meios, rentabilizando o apoio logístico e limitando o número de infraestruturas, aproveitando ao máximo as que se mostrarem mais adequadas" (RCM, 2013b).

Ramo Independente das Forças Armadas – uma arma ou comando independente das FFAA (Department of Defense [DOD], 2021, p.27). De acordo com a Lei Orgânica n.º 6/2014, de 01 de setembro, tem "por missão principal participar, de forma integrada, na defesa militar da República, nos termos do disposto na Constituição e na lei, sendo fundamentalmente vocacionados para a geração, preparação e sustentação das forças da componente operacional do sistema de forças, assegurando também o cumprimento das missões reguladas por legislação própria e das missões de natureza operacional que lhes sejam atribuídas pelo Chefe do Estado-Maior-General das Forças Armadas".

Tecnologias de informação e comunicações – "expressão que designa o conjunto de tecnologias, progressivamente homogéneo, que enformam os actuais sistemas de informação e sistemas de comunicação. Esta expressão reflecte, assim, o processo de convergência tecnológica a que se assiste entre as duas áreas" (Estado-Maior da Armada [EMA], 2006, p. II.372).

Treino – "o Treino das equipas é fundamental, sejam estas operacionais ou de suporte às várias estruturas que participam nas operações, sejam unidades individuais, de grupo ou mesmo alianças internacionais. Só o treino permite aos diversos intervenientes num teatro de operações a resposta pronta e capaz às necessidades estratégicas, operacionais e táticas do comando […] As lições aprendidas através do treino permitem a revisão ou mesmo o desenvolvimento de novos conceitos com impacto direto no aperfeiçoamento das capacidades operacionais" (Neves, 2015, p. 52).

Uniformização da infraestrutura – as infraestruturas são projetadas através da padronização de interfaces e protocolos, e através da difusão dos vários componentes padronizados, sendo um pré-requisito para o desenvolvimento de serviços e aplicações baseadas nessa infraestrutura. A uniformização é, portanto, um objetivo de gestão para o portfolio das Tecnologias da Informação, juntamente com integração, flexibilidade e agilidade, custos marginais reduzidos e custo reduzido ao longo do tempo (Ebbesson & Olsson, 2008).

Apêndice B - Conceção metodológica da investigação

Tema: Edificação de um Ramo independente das FFAA para o domínio do ciberespaço							
Objetivo Geral: Avaliar a adequabilidade de edificação de um Ramo independente das FFAA, com capacidade de atuar no domínio do ciberespaço, integrando tudo o que é comum nas FFAA no quadro dos sistemas de informação e comunicações.							
Objetivos Específicos		**Questão Central:**	Será adequado edificar um Ramo independente das FFAA com capacidade para aturar no domínio do ciberespaço?	**Conceito**	**Dimensão**	**Indicadores**	**Técnicas de Recolha**
OE1	Analisar a atual capacidade militar das FFAA para atuar no domínio do ciberespaço.	**QD1**	Qual a atual capacidade militar das FFAA para atuar no domínio do ciberespaço?	Capacidade Militar	Estratégica	Doutrina Organização Treino Material Liderança Pessoal Infraestruturas Interoperabilidade	Análise documental Entrevistas semiestruturadas
OE2	Identificar os contributos para a capacitação militar, decorrentes da edificação de um Ramo independente das FFAA com capacidade de atuar no domínio do ciberespaço.	**QD2**	Quais as forças, fraquezas, oportunidades e ameaças decorrentes da edificação de um Ramo independente das FFAA com capacidade de atuar no domínio operacional do ciberespaço?	Ciberespaço Racionalização de recursos	Estratégica	Forças Fraquezas Oportunidades Ameaças	Entrevistas semiestruturadas

Apêndice C - Missão e atribuições do Centro de Ciberdefesa (*draft*)

Conforme Regulamento Interno (CCD, 2020), a missão e atribuições do Centro de Ciberdefesa são:

a. O Comando de Ciberdefesa das Forças Armadas assegura o exercício do planeamento, treino operacional e comando operacional das forças e meios de ciberdefesa das Forças Armadas, pelo CEMGFA, em todo o tipo de situações e para as missões das FFAA, bem como a ligação com as forças e serviços de cibersegurança de outros organismos do Estado e nações Aliadas, no âmbito das suas atribuições.

b. O CCD tem por missão assegurar o exercício, pelo CEMGFA, do comando operacional das forças e meios de ciberdefesa das FFAA, em todo o tipo de situações e para as missões das FFAA.

c. Tem ainda por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das FFAA e no âmbito da cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação do restante universo da defesa nacional.

d. O CCD prossegue, no âmbito das competências do CEMGFA, as seguintes atribuições:
   (1) Planear o emprego e conduzir, ao nível estratégico e operacional, as operações de ciberdefesa nos planos externo e interno;
   (2) Estudar e coordenar a implementação de medidas tendentes a assegurar a capacidade de ciberdefesa nas Forças Armadas;
   (3) Assumir a direção e coordenação da capacidade nacional de ciberdefesa;
   (4) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a ciberdefesa e para a cibersegurança setorial da defesa nacional;
   (5) Assegurar a coordenação e o trabalho colaborativo e integrado com os NCIRC dos ramos das FFAA e do EMGFA;
   (6) Contribuir para as Operações de Informação, na vertente *Computer Network Operations*;
   (7) Manter atualizada uma carta de conhecimento situacional do ciberespaço no domínio das Forças Armadas;
   (8) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço, no âmbito da cibersegurança setorial da defesa nacional;
   (9) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com os *Computer Incident Response Capability* (CIRC) nacionais e internacionais, de forma articulada com as competências de coordenação da cooperação nacional e internacional do CNCS;
   (10) Cooperar com as estruturas nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.
   (11) Acompanhar a projeção e a retração de forças nacionais destacadas efetivando a capacidade de ciberdefesa das mesmas;
   (12) Planear e dirigir o treino operacional conjunto no âmbito da ciberdefesa;
   (13) Disponibilizar, e coordenar a capacidade de ciberdefesa no emprego de forças e meios da componente operacional do sistema de forças nas missões reguladas por legislação própria e em outras missões de natureza operacional que sejam atribuídas aos ramos das Forças Armadas, no quadro de um relacionamento permanente com os comandos de componente;
   (14) Acompanhar, no âmbito da ciberdefesa, a participação dos militares das FFAA destacados no exterior, designadamente em atividades decorrentes da satisfação de compromissos internacionais, incluindo a cooperação técnico-militar no âmbito dos compromissos decorrentes do respetivo programa quadro e em outras atividades no âmbito da Comunidade dos Países de Língua Portuguesa (CPLP);
   (15) Planear e coordenar o emprego operacional das forças e meios da ciberdefesa das FFAA em ações coordenadas com CNCS;
   (16) Assegurar a ciberdefesa dos sistemas que permita garantir a capacidade de comando e controlo do CEMGFA, da sua estrutura operacional;

e. Para os efeitos previstos nos números anteriores, o CCD relaciona-se em permanência com os comandos de componente dos ramos, incluindo para as tarefas de coordenação administrativa-logística, sem prejuízo das competências próprias dos Chefes de Estado-Maior dos ramos.

Apêndice D - Resumo da Entrevista - Marinha

DATA	07 de maio de 2021
ENTREVISTADO	CFR EN-AEL Francisco Câmara de Assunção
PERSPETIVA	Marinha

1) Breve caracterização da organização atual e capacidade para atuar no domínio do ciberespaço.

De acordo com o disposto no DR n.º 13/2015, é definido que compete ao CCD conduzir operações militares no ciberespaço, assim como assegurar a coordenação e o trabalho colaborativo e integrado com os NCIRC dos Ramos das FFAA e do EMGFA.

A condução de operações no ciberespaço compete ao CCD, que se encontra integrado na DIRCSI, sob a alçada do EMGFA, sendo esta a responsável pela coordenação das Operações CISIO (*Communication and Information Systems Infrastructure Operations*) – Operações Correntes de deteção, mitigação e recuperação de sistemas, bem como operações de prevenção, tais como análise de vulnerabilidades, *patching*, campanhas de *awareness*, configuração de sistemas, etc.

Para a execução de operações que impliquem uma atuação no ciberespaço exterior ao segmento das FFAA, o CCD responde diretamente ao CEMGFA, ou seja, mesmo que em resposta a uma ação provocada por um ator externo, se vamos tomar medidas defensivas que possam influenciar a atuação desse ator no ciberespaço, estas ações serão coordenadas pelo CEMGFA.

Os NCIRC dos Ramos e EMGFA (que não se encontra implementado, sendo as suas tarefas assumidas pelo CCD) apenas têm autonomia para efetuar Operações CISIO, ou seja, Operações Correntes de deteção, mitigação e recuperação de sistemas, e funcionam como satélites do CCD para monitorizar e defender o segmento de rede nacional que lhes está atribuído.

Na Marinha, o NCIRC encontra-se na Direção de Tecnologias da Informação e Comunicações (DITIC), que por sua vez se encontra sob a alçada da Superintendência das Tecnologias da Informação (STI). Ao nível do Estado-Maior da Armada, a Ciberdefesa e Tecnologias de Informação e Comunicações encontra-se integrada na Divisão de Operações.

2) Principais preocupações/limitações do atual modelo de implementação da ciberdefesa.

Para o EMGFA, a existência de uma estrutura descentralizada das TIC faz com que seja necessária a existência dos NCIRC dos Ramos, uma vez que irão contribuir para uma melhor interligação com as respetivas direções de TIC. Caso não existissem os NCIRC, seria bastante mais difícil garantir uma eficaz interligação.

Recursos Humanos: O CCD encontra-se dependente da disponibilidade dos Ramos para recrutar e fornecer recursos humanos para a capacitação da ciberdefesa, sendo que os próprios Ramos não dispõem desses recursos, nem em quantidade, nem com as respetivas competências, o que é uma grande limitação, uma vez que se torna difícil garantir uma correta captação de talentos, bem como a sua retenção no CCD e nas FFAA.

Formação: Pessoal disponibilizado pelos Ramos sem a formação necessária, sendo necessário o CCD administrar a formação necessária durante o decurso do desempenho de funções.

Material: A grande heterogeneidade de arquiteturas de rede, sistemas e tecnologias nas FFAA, bem como a obsolescência do material dificultam uma resposta defensiva e colaborativa dos sistemas das FFAA.

Doutrina: A falta de *Rules of Engagement* e normativo atualizado ao nível do EMGFA e dos Ramos é uma limitação identificada, estando atualmente a ser desenvolvido um esforço pelo EMGFA para a elaboração de doutrina conjunta para as operações no ciberespaço, que deverá ser materializada no normativo interno do CCD e dos Ramos.

Liderança: Através do DR n.º 13/2015, compete ao CCD assumir a direção e coordenação da capacidade nacional de ciberdefesa, no entanto, não existe nenhum normativo que estabeleça uma relação funcional entre o CCD e os NCIRC dos Ramos.

Interoperabilidade: Através do DR n.º 13/2015, compete ao CCD assegurar a coordenação e o trabalho colaborativo e integrado com os NCIRC dos ramos das FFAA e do EMGFA, bem como partilhar a informação numa estratégia de resposta defensiva e colaborativa com o CNCS e os CIRC nacionais e internacionais.

3) Comparando a organização e capacidade militar atual de Portugal com a de outros países constituintes da UE e da OTAN, considera que algum dos modelos adotados por esses países possa ser adaptado à realidade nacional, trazendo claros benefícios?

Um bom modelo de organização para a cibersegurança é o adotado pela Alemanha, com a criação do *Cyber and Information Domain Service* (CIDS) que contempla um Comando Ciber, uma estrutura CIS e uma célula de Intel, no entanto, não tem uma aplicação direta à dimensão e realidade nacional. É preciso estar atento ao que se pretende com este Serviço, pois é importante perceber que a Alemanha junta neste serviço dois domínios de extrema importância que podem surgir par-a-par, o domínio da Ciber e o domínio da Informação. Não se pode neste caso menosprezar o domínio da informação, os alemães fazem questão de juntar estes dois pela sua interdependência.

4) **Considera que com a mudança de paradigma para uma unificação/centralização da capacidade de ciberdefesa, e para que esta tenha capacidade de atuação plena, se torna necessário integrar e centralizar também toda a gestão dos sistemas de TIC das FFAA?**

Sim, uma vez que esta centralização irá contribuir para a racionalização de recursos, economia de escala, e para a uniformização de tecnologias e processos.

Numa perspetiva Operacional, para que possa haver uma eficaz alteração da atual estrutura distribuída para uma estrutura centralizada dos NCIRC, a mudança terá de ser mais profunda que simplesmente a componente da ciberdefesa, sendo necessário unificar e centralizar a gestão de todas as redes dos Ramos, de modo a ser possível ter um conhecimento alargado das redes que permita avaliar as ameaças e isolar os falsos positivos.

Deste modo, deverá haver primeiramente uma unificação das TIC e homogeneização da arquitetura de rede e tecnologias utilizadas para depois se poder unir os NCIRC.

5) **Considera que a integração e centralização da gestão dos sistemas de TIC das FFAA é possível de encaixar na atual estrutura orgânica do EMGFA? Onde se poderia encaixar? O que seria necessário alterar? Como poderiam ser geridos os recursos atualmente existentes (material e pessoal)?**

Considero ser possível centralizar a capacidade de ciberdefesa e integrar a mesma na estrutura do EMGFA, no entanto, essa capacidade, que é uma capacidade operacional, deveria sair da alçada da DIRCSI, que é uma Direção Técnica, e passar a estar sob um comando Operacional, ou mesmo, ser criado um Comando Ciber na direta dependência do CEMGFA, da mesma forma que acontece com os restantes comandos Operacionais existentes ao nível dos Ramos, tal como o Comando Naval, Comando Aéreo ou Comando das Forças Terrestres. Quanto às TIC, poderiam ser integradas de forma centralizada na DIRCSI.

No eventual processo de centralização das capacidades e infraestruturas tecnológicas, é fundamental que os recursos humanos existentes nos Ramos integrem a nova capacidade conjunta, permitindo fazer uma transição suave e ao mesmo tempo manter a ligação e conhecimento das especificidades de cada Ramo. Essa centralização, poderá eventualmente levar à redução de recursos humanos na vertente de Estado-Maior e Tecnológica, uma vez que estas capacidades se encontram atualmente distribuídas pelos Ramos.

6) **Quais seriam as principais vantagens e desvantagens ao nível da autonomia dos Ramos, capacidade de resposta e qualidade de serviço prestado?**

Apesar de haver um maior afastamento entre a equipa de suporte e o utilizador final, relativamente à atual estrutura distribuída, se houver um correto número de técnicos de suporte, um eficiente sistema de *ticketing*, bem como equipas de intervenção rápida constituídas por elementos com conhecimento das principais particularidades de cada Ramo, é possível que se possa até verificar melhorias na qualidade do serviço prestado.

7) **Considera a edificação de um Ramo independente das FFAA para o domínio da ciberdefesa <u>exequível</u>, <u>praticável</u> e <u>adequada</u> para a dimensão nacional?**

De momento não, dado o enorme investimento necessário a nível económico, e sobretudo a quantidade de recursos humanos que seriam necessários para garantir toda uma estrutura de comando e suporte a esse Ramo, sendo que considero que deva manter-se debaixo da alçada do CEMGFA.

8) **Quais os principais Contributos/Vantagens para a capacitação militar, decorrentes da centralização de recursos materiais e pessoais na estrutura do EMGFA?**

A alteração da atual estrutura distribuída para uma estrutura centralizada de ciberdefesa sob a alçada do CEMGFA terá como principal vantagem uma organização mais simples, garantindo uma doutrina única e transversal às FFAA. Embora atualmente, ao nível das tecnologias e infraestruturas exista uma grande heterogeneidade no seio das FFAA, deve-se caminhar para a sua homogeneização, o que irá facilitar a interoperabilidade, não só nas tarefas de administração, gestão e defesa da rede, mas também irá permitir incrementar o treino do pessoal, criar políticas/configurações de segurança e gerar modelos de deteção de ameaças mais ricos, contribuindo para aumentar a robustez e resiliência das redes das FFAA contra ciberataques.

Ao nível do pessoal, o recrutamento é a parte mais crítica, sendo que o modelo de recrutamento e seleção deverá ser ajustado às necessidades específicas desta componente, através de testes psicotécnicos específicos para a área da ciberdefesa/cibersegurança. Ao nível dos Oficiais, deverá haver uma menor rotatividade e deverá ser ministrada formação a um nível mais teórico e abrangente, sendo que ao nível dos Sargentos e Praças, deverá haver uma maior rotatividade e a sua formação deverá ser mais técnica e específica para as funções a desempenhar. Deverá ainda haver a capacidade de tornar o recrutamento de civis apelativo, face ao mercado de trabalho nacional, de modo a ser possível captar talentos que se venham a tornar uma mais-valia para a capacitação da ciberdefesa nacional.

Apêndice E - Resumo da Entrevista - Força Aérea

DATA	12 de maio de 2021
ENTREVISTADO	TCOR TINF António Jorge Valente
PERSPETIVA	Força Aérea

1) Breve caracterização da organização atual e capacidade para atuar no domínio do ciberespaço.

Do ponto de vista ciber, a FA tem uma secção, a sub-repartição de ciberdefesa, integrada na repartição de Tecnologias de Informação, que o que faz na realidade é cibersegurança, ou seja, faz a segurança de perímetro e proteção das redes da FA. Esta estrutura técnica encontra-se em expansão, e está dependente de uma direção técnica, a DCSI, que se encontra sob o Comando da Logística. Do ponto de vista técnico, é responsável pelos equipamentos de perímetro, ou seja, tem várias funções, de entre as quais a sensibilização do ponto vista da formação, e a administração e aplicação de regras em equipamentos de perímetro, seja perímetro externo, entre ramos ou entre unidades.

A nível de Estado maior, sob a dependência direta do Subchefe do Estado-Maior da FA, a Divisão de Comunicações e Sistemas de Informação tem uma entidade denominada coordenador da ciberdefesa para a FA, que é na prática, quem estabelece a ponte entre o Estado-Maior da FA, do ponto de vista estratégico, e a direção técnica, e é também o interlocutor com os outros Ramos e com o EMGFA. Do ponto de vista técnico e funcional, o NCIRC fala diretamente com o CCD e com os Ramos, mas do ponto de vista formal, e ao nível estratégico, é esta a divisão que que estabelece essa ligação.

2) Principais preocupações/limitações do atual modelo de implementação da ciberdefesa.

Recursos Humanos: Do ponto de vista de recursos humanos, existe um problema na obtenção de recursos humanos qualificados, e com esta dificuldade, manter capacidades autónomas diferentes dispersas pelos vários Ramos não será a melhor opção. Neste modelo, não temos atratividade do ponto de vista financeiro para reter os recursos humanos mais qualificados, especialmente se tivermos a falar das áreas mais específicas da ciberdefesa, nomeadamente *penetration testing*, ataque, ou desenvolvimento de armas ciber. Por outro lado, demora muitos anos a formar um elemento e a ganhar proficiência. A questão da formação base e dos requisitos de progressão na carreira são outro entrave (mais nuns Ramos, que noutros). Não haver progressão horizontal dificulta, uma vez que as pessoas não poderão fazer as tarefas técnicas ao longo de toda a carreira. O desafio do Pessoal, de entre todos, é aquele que não aparenta ter uma solução óbvia e simples.

Formação: A formação não parece um problema difícil, uma vez que é uma questão financeira. Atualmente já existe formação, mas vai ser necessário trabalhar muito nesta área, porque a formação pode ir até um certo ponto, mas no momento em se quiser avançar para a produção de armas autónomas, para usar vantagem no ciberespaço, a formação é necessária, mas o treino e capacidade também são importantes.

Material: Está muito relacionado com as realidades dos Ramos, portanto, efetivamente temos uma infraestrutura e temos tecnologias que são muito heterogéneas, distribuídas, e que têm diferentes políticas, sendo que isso não ajuda os esforços de proteção das infraestruturas. Pensando na ciberdefesa como proteção das infraestruturas, haverá alguns desafios, mas não tão desafiantes como o desafio ao nível do pessoal.

Doutrina: Neste momento não temos um problema a meu ver. Apesar de cada Ramo ter a liberdade de emanar doutrina própria, se houver diretivas, ou se houver uma estratégia de ciberdefesa, de que derivem diretivas e planos, isso vai construir outro edifício doutrinário que vai permitir um melhor funcionamento.

Liderança: O fato do CCD estar enquadrado dentro de uma direção no EMGFA serve até um determinado ponto, mas depois a importância da ciberdefesa irá continuar a aumentar (é o que eu acredito que vá acontecer) e naturalmente, de alguma forma a liderança, vai ter que alterar para não estrangular a ciberdefesa. Neste momento, a ciberdefesa continua a ser vista como um problema de J6 (Informática), e não é, especialmente porque estamos a observar como a ciberdefesa se está a tornar a nova área de operações para as FFAA e para os conflitos. Eventualmente terá de ser estudado se a ciberdefesa deverá continuar a ser CSI, ou se deve mudar para uma componente operacional como por exemplo o CCOM, ou um comando separado.

Interoperabilidade: A constituição dos NCIRC permite a interoperabilidade entre os Ramos e o CCD, e a interoperabilidade com as entidades externas é efetuada de forma centralizada através do CCD.

3) Comparando a organização e capacidade militar atual de Portugal com a de outros países constituintes da UE e da OTAN, considera que algum dos modelos adotados por esses países possa ser adaptado à realidade nacional, trazendo claros benefícios?

Um dos modelos que eu acho interessante, é o alemão. Na capacidade defensiva as lições estão aprendidas e existe muita coisa para podermos avançar sem precisar de olhar para as estruturas dos outros, sendo que todos tem os mesmos desafios. O desafio dos recursos humanos é transversal a toda a Europa e toda a OTAN. É muito difícil qualquer organismo público pagar o que os privados estão a pagar neste momento. Do ponto de vista ofensivo, há uma visão romântica de que podemos contratar pessoal com as competências, ou melhor, podemos coordená-los, não necessitando estes de serem militares. No entanto, é complexo do ponto de vista doutrinário. Fazendo um meio termo, pode-se comprar armas cibernéticas e ter pessoal com competências para

operar essas armas desenvolvidas por terceiros. Este é o modelo que considero mais viável se quisermos ter alguma capacidade. Mas se quisermos desenvolver as nossas próprias armas, vai ser mais complexo, sendo que este domínio não é comparável diretamente com a Marinha, Exército e FA.

4) **Considera que com a mudança de paradigma para uma unificação/centralização da capacidade de ciberdefesa, e para que esta tenha capacidade de atuação plena, se torna necessário integrar e centralizar também toda a gestão dos sistemas de TIC das FFAA?**

Posso considerar que para que se centralize a ciberdefesa, tem que ficar claro o papel da ciberdefesa do ponto de vista de entidade que emana instruções, e deverá ter capacidade coerciva para garantir o cumprimento das instruções por si emanadas. Não considero correto juntar a ciberdefesa com as TIC. No entanto, não vejo desvantagem nenhuma na centralização da ciberdefesa e na centralização das TIC, só vejo vantagens a nível de pessoal, recursos, licenciamento e economia de escala, mas é um processo que terá de ser feito de forma gradual e concertada. Sendo que deste modo, já deveríamos ter iniciado o processo, que do ponto de vista da cibersegurança seria benéfico, pois tornaria muito mais simples a aplicação de políticas de gestão transversais.

5) **Considera que a integração e centralização da gestão dos sistemas de TIC das FFAA é possível de encaixar na atual estrutura orgânica do EMGFA? Onde se poderia encaixar? O que seria necessário alterar? Como poderiam ser geridos os recursos atualmente existentes (material e pessoal)?**

Neste momento não considero que se possa encaixar na atual estrutura orgânica, a DIRCSI teria de ganhar mais força, julgo que deveria ter um Oficial no mínimo de 2 estrelas. Eventualmente poderia ter que mudar para uma componente mais operacional como por exemplo o CCOM, ou um comando separado.

6) **Quais seriam as principais vantagens e desvantagens ao nível da autonomia dos Ramos, capacidade de resposta e qualidade de serviço prestado?**

Considero que melhorava tudo, se for bem feito, mas se for mal feito só tem desvantagens. Tem todo o potencial para melhorar, mas é preciso ter uma boa comunicação para dentro dos ramos, ou seja, os mecanismos de apoio e de distribuição, e seja de apoio logístico, seja de apoio de suporte ao serviço, seja de distribuição de máquinas, seja de substituição de equipamentos, faz com que provavelmente grande parte da infraestrutura de apoio que existe nos Ramos atualmente terá que se manter nos Ramos para suporte básico. Se o modelo e os mecanismos não forem bem implementados, pode trazer uma eventual perda de autonomia dos Ramos, com impacto direto na celeridade dos processos.

7) **Considera a edificação de um Ramo independente das FFAA para o domínio da ciberdefesa <u>exequível</u>, <u>praticável</u> e <u>adequada</u> para a dimensão nacional?**

Não praticável, nem adequada, nem exequível. Neste momento, não acho que seja necessário a edificação de um ramo independente, porque supõe uma série de características que neste momento não se justificam, ou seja, pretende-se que a capacidade seja dinâmica, eficaz e talvez daqui a alguns anos ou décadas, faça sentido. Neste momento, não faz. Eu estou a falar na questão nacional, eventualmente lá chegaremos, mas vai demorar décadas, porque neste momento não existe sequer a maturidade suficiente. Vejo, por exemplo, um comando com um oficial general, se calhar diretamente muito próximo do centro de comando. Um pouco à semelhança de como as forças especiais estão para as forças armadas, mas sem estar preso a nenhum Ramo. Uma espécie de força especial, mas que em vez de estar ligada a um Ramo, se encontre debaixo da alçada do CEMGFA.

8) **Quais os principais Contributos/Vantagens para a capacitação militar, decorrentes da centralização de recursos materiais e pessoais na estrutura do EMGFA?**

<u>Organização:</u> Do ponto de vista da ciber ganhamos, do ponto de vista das TIC é discutível, mas ganha-se ao tornar a organização mais simples.

<u>Recursos Humanos:</u> É de caras a grande vantagem da centralização. Com base na centralização pode-se chegar-se à conclusão que os Ramos têm de adaptar as suas carreiras e criar uma carreira na área do saber das comunicações e sistemas de informação, permitindo uma menor rotatividade nos cargos técnicos.

<u>Formação:</u> Não se pode entrar pela base e começar logo na ciber, porque se não tiver conhecimento de redes e sistemas, é difícil exercer ciber. Deverá ter uma experiência base na área das TIC.

<u>Material:</u> É obvia a vantagem em termos de homogeneidade e economia de escala.

<u>Doutrina:</u> É obvia a vantagem da centralização na sua homogeneização, porque por muito que seja emanada doutrina pelo EMGFA, os Ramos serão sempre independentes para aplicar, ou não, essa doutrina.

<u>Infraestruturas:</u> A gestão centralizada de todas as redes é excelente, mas tem o desafio dos problemas específicos de cada Ramos, podendo ser necessário numa fase inicial adaptar as equipas de modo a ter elementos de um Ramo a trabalhar para o seu Ramo para a execução de tarefas específicas, e para tarefas mais genéricas, poder existir equipas diversificadas.

<u>Treino:</u> Reduz-se a quantidade de pessoal que é necessário treinar e formar. Assim como existe atualmente uma escola em cada Ramo para dar formação na área das TIC, sendo que estas capacidades poderiam ser centralizadas, sobretudo quando houver uma homogeneização de material.

<u>Liderança:</u> A única desvantagem do comando e controlo centralizado é não ter o recurso próximo do Ramo.

<u>Interoperabilidade:</u> Não irá haver grande alteração, pois os Ramos interagem apenas entre si. Para fora, a interação é efetuada pelo CCD.

Apêndice F - Resumo da Entrevista - Centro Nacional de Cibersegurança

DATA	14 de maio de 2021
ENTREVISTADO	CALM EME RES António Gameiro Marques
PERSPETIVA	Centro Nacional de Cibersegurança

1) Breve caracterização da organização atual e capacidade para atuar no domínio do ciberespaço.

Na atual Lei Orgânica do EMGFA, o CCD encontra-se debaixo da DIRCSI para operações correntes, no entanto já está contemplada a possibilidade de em operações militares, o comando do CCD ficar debaixo do CCOM, portanto, é necessário ter em atenção a organização para operar no ciberespaço. A lógica é a DIRCSI criar a capacidade, que posteriormente é utilizada pelo CCOM para operações militares no ciberespaço.

2) Comparando a organização e capacidade militar atual de Portugal com a de outros países constituintes da UE e da OTAN, considera que algum dos modelos adotados por esses países possa ser adaptado à realidade nacional, trazendo claros benefícios (modelos ao nível estratégico, que possam beneficiar o relacionamento da componente militar com a componente civil)?

As FFAA portuguesas devem ter como nível de ambição, reforçar de forma muito significativa a capacidade de ciberdefesa nacional através das FFAA, e devem inclusivamente olhar cada vez mais, e tratar cada vez mais aquela área como uma área de operações militares, como preconiza o Sr. COR TM Viegas Nunes (Nunes, 2020) no seu trabalho de investigação, tal como se faz para as operações navais, aéreas e terrestres.

Poderão ter uma abordagem a 2 passos. 1º nível, estabilizar o que hoje existe. 2º nível adquirir armas cibernéticas e estar capaz de as utilizar, com Conceito de Operações (CONOPS), *Operational Tasking* (OPTASK), e tudo o resto que se aprende nas Operações. Depois, com um outro nível de ambição, ganhar competências para fabricar armas cibernéticas, que está ao nosso alcance. Países como o Vietnam produzem armas cibernéticas e estão atualmente bastante ativos, mas para isso é necessário haver Doutrina, porque tem de se saber muito bem para que é que se vai usar essas armas cibernéticas, e que tipo de armas cibernéticas é que são. E isso é algo que deverá ser desenvolvido em Conceitos de Operações.

3) Considera que com a mudança de paradigma para uma unificação/centralização da capacidade de ciberdefesa, e para que esta tenha capacidade de atuação plena, se torna necessário integrar e centralizar também toda a gestão dos sistemas de TIC das FFAA?

A ciberdefesa, caso saia debaixo da alçada da DIRCSI, deverá ir para a área operacional, debaixo do CCOM, no entanto o Estado-Maior que apoia o General CCOM, terá de ter capacidade para utilizar operacionalmente aquele meio (ciberdefesa) em todas as vertentes do OODA *loop* (*Observ, Orient, Decide and Act*). Se para fazer isto implica criar um novo Ramo, eu tenho dúvidas, pelo menos neste momento, isto é, deve criar-se a capacidade com todas as suas componentes militares como o Sr. COR TM Viegas Nunes (Nunes, 2020) preconiza (uma diretiva de operações e inclusivamente ter a ambição para criar armas cibernéticas) o CCD só se diferenciará do CNCS, quando tiver essa capacidade. E quando tiver essa capacidade, as outras entidades vão olhar para eles com outros olhos.

4) Considera a edificação de um Ramo independente das FFAA para o domínio da ciberdefesa <u>exequível</u>, <u>praticável</u> e <u>adequada</u> para a dimensão nacional?

A resposta à sua pergunta é um "sim, mas". Não concordo que agora em 2021 se inicie um processo de criação de um novo Ramo, não concordo, porque ainda há caminho a fazer até isso acontecer. Deveremos caminhar para esse objetivo, mas ainda há um longo caminho a percorrer antes de lá chegar. É um objetivo que acho que não deve ser alcançado já, porque isso iria criar uma fratura muito grande. Parte desse caminho poderá passar pela reorganização da atual estrutura, eventualmente passando o CCD para debaixo do CCOM, no entanto terá de ser garantido que o CCOM disponha de capacidade de Estado-Maior para operar com a capacidade de ciberdefesa. Tem de se fazer uma reestruturação coerente, "não basta agarrar num bloco e colocá-lo noutro sítio", o próprio Estado-Maior do CCOM tem de ter uma área que pense Ciber, faça OPTASK Ciber, etc… Se queremos encarar isto como uma área de operações militares, temos de construir de forma correta, e acho que estamos na altura de fazer isso. Isso poderá ser o caminho para daqui a alguns anos poder haver um Ramo, o que mesmo assim considero difícil, porque receio que os recursos para as outras missões de natureza física que as FFAA têm de realizar, drenem os recursos humanos.

Concordo que devem ser dados passos no sentido da ciberdefesa ser de facto encarada como um domínio das Operações militares em toda a sua plenitude. Com o quadro doutrinário, com conceito de operações, com uma OPTASK de ciberdefesa, e com um conceito estratégico militar para a ciberdefesa (que deveria ser o primeiro documento a ser feito), e tudo o resto. Porque é daí que depois decorrem os *Requirements*.

5) Quais os principais Contributos/Vantagens para a capacitação militar, decorrentes da edificação de um Ramo independente das FFAA com capacidade de atuar no domínio do ciberespaço, ou centralização de recursos materiais e pessoais na estrutura do EMGFA?

A capacitação seria uma mais-valia para a segurança do ciberespaço de interesse nacional, até porque a estratégia nacional não se chama estratégia nacional de cibersegurança, chama-se estratégia Nacional de segurança do ciberespaço, e é uma estratégia geral para a segurança do ciberespaço que depois pode ter estratégias particulares, e o Ministério da Defesa já está numa fase muito adiantada de produzir uma estratégia nacional de ciberdefesa, para a qual, tanto o CNCS, como o CCD, deram grandes contributos.

Julgo que quem beneficiaria sobretudo seria Portugal, por dispor de uma capacidade mais robusta e mais credível. Eu acho que está na altura, sinceramente, já temos o CCD desde 2015, vai fazer 6 anos, o CNCS é de 2014, vai fazer 7 anos, e já está na altura de dizer: "E agora, qual é a fase seguinte? Qual é o destino?".

Apêndice G - Resumo da Entrevista - Centro de Ciberdefesa

DATA	11 de junho de 2021
ENTREVISTADO	CFR M Sérgio Ricardo Caldeira de Carvalho
PERSPETIVA	Centro de Ciberdefesa

1) Breve caracterização da organização atual e capacidade para atuar no domínio do ciberespaço.

Atualmente temos o CCD sobre um comando técnico, a DIRCSI, que é como a grande maioria dos países que conheço começaram. Normalmente, o Ramo de ciberdefesa nasce numa componente da Segurança da Informação no diretorado CSI das várias nações, mas rapidamente, quando ganha a capacidade operacional e o reconhecimento como um domínio operacional, normalmente nessas nações salta de baixo do comando técnico e passa para o comando operacional, no entanto, em Portugal ainda não demos esse salto, mantendo o CCD debaixo de um comando técnico, que é a DIRCSI. Segundo o ADJPC, a intenção é manter assim, porque não vê razão para ir para o CCOM, no entanto, o Sr. almirante CEMGFA já tem uma visão um pouco diferente, e já vê o CCD como parte integrante do CCOM, pelo menos espera que a parte das operações fiquem sob a alçada do CCOM. O senhor Ministro da Defesa Nacional também já fez saber que espera que a evolução do CCD seja para um comando independente da ciberdefesa. Portanto temos aqui 3 visões completamente diferentes e dispares. Pessoalmente, concordo mais com Sr. Ministro, porque acho que devemos tratar a ciberdefesa como um verdadeiro domínio operacional, o que ainda não fazemos, por que continuamos a utilizar a ciberdefesa como suporte para a missão, e não para alcançar a missão, o que para mim está completamente errado. É o tal pulo, de ser um domínio operacional, e quando passa a ser um domínio em pé de igualdade com os outros domínios, tem de contribuir para cumprir com os objetivos da missão. Acho que esse passo é importante, e para estarmos em pé de igualdade com os outros organismos de ciberdefesa na Europa e nos países aliados em geral, teremos de ter um comando de ciberdefesa, neste momento somos dos poucos países que não tem um comando de ciberdefesa.

A capacidade ofensiva no ciberespaço, de uma maneira muito simplista, é a capacidade de provocar efeitos no ciberespaço, e como os Espanhóis dizem, e muito bem, se não existe capacidade ofensiva não se tem ciberdefesa, tem-se apenas de cibersegurança.

Atualmente, a nível nacional, existe uma matriz de regras de empenhamento baseada nos diversos tipos de operações baseada na taxonomia OTAN definida, mas que ainda não se encontra aprovada, estando em análise a sua aprovação, devido à sensibilidade do assunto em questão.

2) Principais preocupações/limitações do atual modelo de implementação da ciberdefesa.

Pessoal: Nós temos muita falta de pessoal na ciberdefesa, é o nosso principal problema. Atualmente devíamos ser 90 elementos no CCD e somos 33, e os ramos não têm mais pessoal para colocar no CCD, e todos os que lá colocarem é com sacrifício próprio, porque não existe pessoal técnico desta área suficiente. Existe uma enorme dificuldade porque além de serem poucos, há muito pessoal a sair das FFAA, porque o mercado de trabalho é extremamente aliciante, e nós não temos capacidade para competir com o mercado.

Material/Infraestruturas/Tecnologias: Felizmente, neste momento, ainda não falta dinheiro para a aquisição do material e infraestrutura tecnológica necessária, pelo que não me parece ser uma preocupação.

Doutrina: Está a ser desenvolvido, e vai ser enviado oficialmente aos Ramos dentro de curto prazo uma publicação doutrinária militar conjunta, para estes comentarem e darem contributos. Estão também a ser elaboradas uma série de normas de instrução técnicas para constituir uma base doutrinária mais tática. A nível doutrinário estamos a avançar, e espero que a curto prazo, ainda este ano, se consiga publicar a primeira publicação doutrinária na área da ciberdefesa.

Treino: Temos participado em exercícios, e a grande parte da evolução de procedimentos e necessidade de busca de conhecimento tem resultado dos exercícios internacionais que temos participado e no nosso relacionamento com os outros centros de ciberdefesa e outros profissionais de ciberdefesa da OTAN. Parece-me que o grande catalisador da capacidade de ciberdefesa será a edificação de uma escola, se essa edificação for de acordo com aquilo que está planeado, que é através da contratação do serviço de uma empresa de *capacity building* de ciberdefesa para edificação da escola.

Liderança: Para mim, a liderança de topo tem que ser operacional e a liderança específica tem que ser técnica, o que não quer dizer que no futuro a liderança não possa ser feita por um elemento técnico com experiência de ter efetuado operações no ciberespaço. Mas neste momento acho que temos que ir buscar pessoal com visão operacional e capacidade de liderança de equipas.

Interoperabilidade: Ao nível da ciberdefesa, isto é, equipamentos de segurança de perímetro e plataformas de segurança, acaba por haver interoperabilidade, uma vez que é o CCD que fornece grande parte dos sistemas e equipamentos aos Ramos, o que cria uma certa uniformização, já o mesmo não acontece ao nível dos sistemas de TIC, em que cada Ramo é o responsável pela aquisição e escolha dos equipamentos, sistemas e tecnologias, não havendo uma linha orientadora.

Outras Limitações: A edificação da capacidade deveria ter o mesmo chefe durante toda a fase de edificação, uma vez que a troca de chefes, pode causar uma modificação da visão, o que pode levar a uma disrupção na linha orientadora.

A ciberdefesa deveria ser uma componente, na minha opinião. Neste momento ainda existe a visão, por muitos elementos, que a ciberdefesa como algo apenas para os técnicos.

3) **Comparando a organização e capacidade militar atual de Portugal com a de outros países constituintes da UE e da OTAN, considera que algum dos modelos adotados por esses países possa ser adaptado à realidade nacional, trazendo claros benefícios?**

Temos o modelo utilizado pela da Alemanha, se a intenção for a criação de um Ramo independente com o CSI englobado, ou o modelo da Espanha, que também está muito bom para o nível operacional.

4) **Considera que com a mudança de paradigma para uma unificação/centralização da capacidade de ciberdefesa, e para que esta tenha capacidade de atuação plena, se torna necessário integrar e centralizar também toda a gestão dos sistemas de TIC das FFAA?**

Vamos ter sempre de centralizar as TIC, caso contrário vamos ter sempre problemas. No entanto, a ciberdefesa e as TIC não podem estar sob o mesmo chefe, devem estar separados, sempre, porque caso contrário não funciona bem.

Eu acho que devemos ter uma organização, um pouco à semelhança dos alemães, em que a ciberdefesa está separada da segurança e das redes, isto porque alguém tem de validar e auditar aquilo que é feito pelas TIC e pela equipa de segurança, caso contrário, se quem faz a auditoria é o mesmo que aplica as regras, todo o trabalho de validação e auditoria torna-se uma falácia.

5) **Considera que a integração e centralização da gestão dos sistemas de TIC das FFAA é possível de encaixar na atual estrutura orgânica do EMGFA? Onde se poderia encaixar? O que seria necessário alterar? Como poderiam ser geridos os recursos atualmente existentes (material e pessoal)?**

É possível encaixar na estrutura da DIRCSI, mas esta terá de ser muito reforçada, e terá de se dar maior importância à DIRCSI, sendo que os recursos teriam de ser geridos centralmente, tendo em atenção que os Ramos não poderão ficar vazios. No entanto, a gestão centralizada iria levar a que não fosse necessário ter tanto pessoal especializado, podendo haver equipas de resposta que poderiam dar suporte aos Ramos.

6) **Quais seriam as principais vantagens e desvantagens ao nível da autonomia dos Ramos, capacidade de resposta e qualidade de serviço prestado?**

Os Ramos, sem dúvida que irão perder um pouco a sua autonomia, no entanto haverá a vantagem da uniformização, cumprimento e responsabilização, por parte dos Ramos, que levarão sem dúvida a uma maior segurança das redes, e a uma maior cultura de cibersegurança nas FFAA.

7) **Considera a edificação de um Ramo independente das FFAA para o domínio da ciberdefesa <u>exequível</u>, <u>praticável</u> e <u>adequada</u> para a dimensão nacional?**

É sem dúvida exequível, só depende da vontade das pessoas (é apenas uma questão técnica e há a vantagem da racionalização dos meios), no entanto parece-me pouco praticável, pois acredito que haja uma grande resistência à mudança, parece-me que teria de ser imposto para que funcionasse. Para a dimensão nacional, sem dúvida nenhuma que é adequado.

Inicialmente deveríamos passar para um comando e posteriormente para uma componente. Deverá ser efetuado um plano a médio prazo (7 ou 8 anos). Assim que o Comando estiver estabilizado, com a parte formativa e de Recursos Humanos estabilizada, passar para uma componente, garantindo-se a continuidade do pessoal, e muito mais, que não conseguimos garantir com uma carreira na ciberdefesa, se estiver ao nível de um comando.

8) **Quais os principais Contributos/Vantagens para a capacitação militar, decorrentes da edificação de um Ramo independente das FFAA com capacidade de atuar no domínio do ciberespaço, ou centralização de recursos materiais e pessoais na estrutura do EMGFA?**

<u>Organização, Liderança e Recursos Humanos:</u> A nível organizacional, responde diretamente ao CEMGFA e tendo uma estrutura própria vai resolver o problema do pessoal, porque tem a vantagem de ter uma carreira militar dentro de um Ramo. A outra vantagem é ter uma especialização, ao passo que atualmente é complicado conseguir conciliar os requisitos de promoção dos Ramos, com uma carreira na ciberdefesa.

<u>Material:</u> Garante-se uma economia de escala, e que os sistemas são interoperáveis.

<u>Doutrina:</u> Ainda tem de ser edificada doutrina conjunta para a ciberdefesa, mas já se está a iniciar esse processo de edificação. Relativamente à área das TIC, os Ramos já dispõem de doutrina bastante boa, que poderá ser aproveitada, tendo como vantagem a homogeneização de procedimentos.

<u>Treino:</u> Como componente, o treino será levado mais a sério, sendo uma componente que integra em pé de igualdade com os Ramos nos exercícios conjuntos. Nos exercícios internacionais não haverá grande diferença. Outra grande vantagem é ao gerir o treino do pessoal, não se encontra dependente da disponibilidade dos Ramos para que o seu pessoal possa integrar o Treino conjunto.

<u>Infraestruturas:</u> As infraestruturas já existem, eventualmente será necessário arranjar mais algum espaço para albergar um maior número de pessoas, no entanto, já existem algumas instalações que poderiam albergar esse pessoal, que poderão ser utilizadas.

<u>Interoperabilidade:</u> Deixaríamos de ter esta questão, porque estaria tudo centralizado, o que logo à partida irá garantir a interoperabilidade dos sistemas. E junto das entidades externas passaríamos a ter outro peso, porque em vez das entidades externas estarem a interagir com 3 Ramos, estariam a interagir apenas com uma entidade de dimensão e peso superior.

Apêndice H - Resumo da Entrevista - Cooperative Cyber Defence Centre of Excellence

DATA	24 de junho de 2021
ENTREVISTADO	CFR EN-AEL Vasco Marques Prates
PERSPETIVA	Cooperative Cyber Defence Centre of Excellence

1) **Decorrente do normativo vigente (nacional, UE e OTAN) e dos compromissos internacionais assumidos, considera ser necessária a edificação de um Ramo independente das FFAA para o domínio da ciberdefesa para alcançar o nível de ambição nacional a médio prazo?**

Não considero que seja necessário criar um Ramo independente, até porque devemos ter presente a realidade de que Portugal em termos de capital disponível, económico e humano, para edificar algo completamente separado. Considero, portanto, que algo deve surgir numa génese integrada e conjunta. Criar mais um ramo é potenciar as lacunas já existentes de recursos nos atuais Ramos, onde já se verificam grandes dificuldades para prover as atuais necessidades. É necessário obter uma solução de compromisso visto que a ciberdefesa é uma "componente" multi-domínio, transversal a todas as componentes, Marítima, Terrestre, Aérea ou Espacial.

No entanto, é extremamente importante que o relacionamento da ciberdefesa ultrapasse o plano nacional e alcance o contexto Internacional, nas organizações e nos compromissos assumidos, onde é evidente que uma capacidade de ciberdefesa tem de contemplar obrigatoriamente uma componente ofensiva. Esta componente permite a clara distinção da atuação da Defesa no ciberespaço, e consequentemente obter o mesmo reconhecimento que tem noutros domínios e fornecendo meios para execução da missão. Para tal é incontornável a nossa integração e envolvimento em organismos internacionais, seja aqui no CCDCOE, seja na OTAN, no *Cyberspace Operations Centre* (CYOC), ou através da nomeação de pessoal para cargos como Oficiais de ligação para os assuntos de ciberdefesa, caso contrário há um elevado risco de deixarmos de ser relevantes como parceiros para a ciberdefesa no seio e no conceito de hoje da aliança e amanhã na UE.

2) **Comparando a organização e capacidade militar atual de Portugal com a de outros países constituintes da UE e da OTAN, considera que algum dos modelos adotados por esses países possa ser adaptado à realidade nacional, trazendo claros benefícios?**

Não consigo dizer concretamente qual o melhor modelo a adotar. Constato que há uma predominância em aproximar o conceito a países de igual dimensão, territorial ou humana, no entanto considero que os fatores culturais são extremamente importantes na edificação de modelos, e que a transposição por semelhança "numérica" pode acarretar disfuncionalidades por vezes só visíveis a médio/longo prazo. Do que posso observar, e ao dia de hoje, poderia arriscar em dizer que modelos como da República Checa, ou da Roménia poderiam funcionar, pese embora a sua orientação esteja muito focada pelo posicionamento das suas fronteiras terrestres. Em oposição modelos como o de Espanha, da Bélgica ou o da Holanda, apesar de tentadores pela proximidade e equivalência numérica territorial podem ser verdadeiros desafios. Neste momento, Espanha tem um comando conjunto dedicado à ciberdefesa, designado de comando conjunto do ciberespaço, porque os recursos (económico e humano) assim lho permitem, algo que Portugal não dispõe. Por outro lado, a Bélgica e a Holanda têm modelos com forte ligação à indústria privada, e Portugal não possui esse "alcance" em termos empresariais, e em termos estatais, em abono da verdade, também não tem esse alcance financeiro.

3) **Considera que com a mudança de paradigma para uma unificação/centralização da capacidade de ciberdefesa, e para que esta tenha capacidade de atuação plena, se torna necessário integrar e centralizar também toda a gestão dos sistemas de TIC das FFAA?**

Não. Estamos a falar de domínios distintos, com especialidades distintas, com visões destintas, e que requerem abordagens distintas. Se estivermos a falar em termos de segurança periférica e sensores de rede, isto é, equipamentos que façam a segurança da rede, aí faz sentido centralizar e integrar. No entanto, para as TIC vocacionadas para missões específicas, são necessários sistemas de comunicação e de informação dedicados com prazos de obtenção específicos e por vezes céleres, e isso implica que haja um conhecimento de causa não só técnico, mas da natureza do domínio, para a sua correta implementação. Se vamos concentrar nesta área, somos capazes de perder momento, ou seja, a ideia surge, mas e depois uma elevada inércia decorrente do conjunto de regras que é transversal a todos os outros domínios pode comprometer a especificidade do processo, sujeitando uma ideia especifica a regras administrativas gerais.

4) **Considera que a integração e centralização da gestão dos sistemas de TIC das FFAA é possível de encaixar na atual estrutura orgânica do EMGFA? Onde se poderia encaixar? O que seria necessário alterar? Como poderiam ser geridos os recursos atualmente existentes (material e pessoal)?**

Julgo que a ciberdefesa se deva encaixar no EMGFA, conforme aquilo que já se assiste noutros países, mas deve sair da estrutura em que atualmente está inserida, porque em termos de operações de ciberdefesa, não se compadece estar numa área técnica, e deverá passar para um nível superior, na dependência direta do CEMGFA, assim como está o CCOM, por exemplo. Mas a ciberdefesa não deverá integrar o CCOM, uma vez que o seu tipo de operações são, digamos, "operações correntes", tomemos o exemplo da *Cyberspace Information Surveillance and Reconnaissance Operations* (CISRO), que se desenvolvem diariamente, não são direcionadas a uma missão, mas contribuem através do *Situational Awareness*. No entanto, deverá operar de uma forma natural com o CCOM, para missões específicas, integrando as necessárias considerações de

operações no ciberespaço no planeamento das operações. Em relação às TIC, julgo que se devem manter tal como estão, porque deverá continuar a ser garantida uma capacidade residente no Ramo.

5) **Considera a edificação de um Ramo independente das FFAA para o domínio da ciberdefesa exequível, praticável e adequada para a dimensão nacional?**

Conforme referi anteriormente, a escassez de capital económico e financeiro, compromete a exequibilidade e praticabilidade desse desiderato, Portugal não tem esses recursos, as FFAA debatem-se com o grave problema não só de recrutamento mas também de retenção ao que acresce a necessidade de sustentação e renovação de meios, a criação de um novo Ramo só tenderá, salvo melhor entendimento, a agravar o problema no seu conjunto, tanto que acresce a este "sector das TIC" a forte procura dada a sua expansão e especialização. Tem se ser encontrada uma solução, digamos conjunta, que permita a edificação da capacidade, mas que também possa diminuir a presente situação vivida nas FFAA associada ao recrutamento e retenção, podemos encontrar aqui novas áreas de atratividade.

6) **Quais os principais Contributos/Vantagens para a capacitação militar, decorrentes da edificação de um Ramo independente das FFAA com capacidade de atuar no domínio do ciberespaço, ou centralização de recursos materiais e pessoais na estrutura do EMGFA?**

Doutrina: Necessário criar uma estrutura doutrinária e de diretivas ao nível do EMGFA, que sejam transversais a todos os Ramos, não obstante de que estes depois possam desenvolver internamente doutrina mais específica.
Organização: A estrutura de ciberdefesa deverá ser operacionalizada no EMGFA, porque é uma capacidade do EMGFA. As TIC deverão recorrer a uma geometria variável, isto é, ir buscar recursos e formar os recursos no EMGFA, embora esses recursos desempenhem funções nos Ramos, tal como acontece atualmente na ciberdefesa. Ao nível dos processos de aquisição de material, poderá haver alguma vantagem, caso o processo de aquisição seja executado financeiramente através do EMGFA.
Treino: Deve ser centralizado no EMGFA, porque é onde a capacidade é edificada e gerida, o que não quer dizer que os Ramos não tenham margem de manobra para dar outro tipo de formação, que até poderá ser integrada no modelo preconizado pelo EMGFA. No entanto, o plano de formação deverá ser constituído, edificado e gerido pelo EMGFA. O processo de recrutamento deverá ser efetuado pelos Ramos, bem como a formação base de conhecimento organizacional militar, depois os elementos deverão ser entregues ao CCD que deverá ter capacidade para providenciar a formação específica.
Material: Os sistemas de segurança e sensores deverão estar centralizados no EMGFA, e este é que deverá definir os requisitos, no entanto, para o resto dos sistemas e equipamentos não me parece que deva ser centralizado, por causa das especificidades de cada Ramo. A centralização das máquinas e sistemas de poderá ser vista de duas perspetivas: se por um lado, ter o parque informático homogéneo facilita a gestão e aplicação de regras e correções de segurança, por outro lado, caso se sofra um ataque, este irá disseminar-se de forma mais rápida pela rede; já o inverso, torna a gestão mais complexa, mas no caso de um ataque, acaba por tornar a rede mais resiliente. É algo que tem de ser cuidadosamente avaliado.
Pessoal: O processo de recrutamento deverá ser efetuado pelos Ramos, bem como a formação base de conhecimento organizacional militar e depois os Ramos deverão entregar os elementos ao EMGFA - CCD que deverá ter capacidade para providenciar a formação específica em ciberdefesa.
Liderança: A liderança terá de ser feita pelo EMGFA, aliás, já o é atualmente. O que me preocupa em termos de liderança resulta da necessária interação e agilidade entre o nível político e todas as entidades com responsabilidades no ciberespaço, a coordenação e harmonização das ações no ciberespaço é extremamente importante, a ciberdefesa não se faz de forma isolada. E se não tenho questões relativamente a quem cabe as operações no e através do ciberespaço, também não me restam dúvidas que para o fazer é necessária uma imagem comum partilhada do ciberespaço a que corresponde a um *situational awareness* que é, ou deve ser gerado com o contributo de todos os atores e eventualmente coordenado pela Defesa. Não podemos pensar em proteger os nossos sistemas sem saber atempadamente das ameaças ou incidentes existentes. Para poder conseguir medir em tempo eventuais efeitos que se possam propagar, ou saber que um determinado efeito pode colocar em causa determinados sistemas críticos a nível nacional tem de existir uma partilha de conhecimento e uma gestão centralizada reconhecida a nível político. E se não houver uma liderança clara e forte nestas relações, perde-se metade do caminho.
Infraestruturas: Para além do que já existe, que deve continuar a evoluir, considero que deve haver ainda uma estrutura de formação, que poderá ser interna, ou externa à ciberdefesa para providenciar a formação base específica. As infraestruturas dos NCIRC atualmente existentes, não deverão ser abandonadas, por uma questão de redundância ao CCD em caso de emergência, devendo permanecer em funcionamento de forma *unmanned*.
Interoperabilidade: O mais importante é garantir uma continuidade na participação em fóruns como o *Federated Mission Networking* (FMN), e em exercícios onde isto é treinado, como o *Coalition Warrior Interoperability eXercise* (CWIX), em termos de componentes, mas também de nações. Os exercícios são fundamentais para testar, resultando lições identificadas e posteriormente aprendidas contribuindo para uma edificação "linear" da capacidade. Neles torna-se evidente o quão sincronizado, ou desfasado estamos e como estamos relativamente aos restantes países. Relativamente à interoperabilidade entre o CCD e os Ramos, caso os equipamentos de segurança e sensores sejam adquiridos de forma centralizada pelo EMGFA, não se anteveem problemas de interoperabilidade.