INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO ESTADO-MAIOR CONJUNTO

2021/2022

TII

A EVOLUÇÃO DA RELEVÂNCIA DO CIBERESPAÇO PARA A NATO

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

Bruno Manuel da Silva Pereira

MAJOR, CAVALARIA

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A EVOLUÇÃO DA RELEVÂNCIA DO CIBERESPAÇO PARA A NATO

MAJOR, CAVALARIA Bruno Manuel da Silva Pereira

Trabalho de Investigação Individual do CEMC 2021/22

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A EVOLUÇÃO DA RELEVÂNCIA DO CIBERESPAÇO PARA A NATO

MAJOR, CAVALARIA Bruno Manuel da Silva Pereira

Trabalho de Investigação Individual do CEMC 2021/22

Orientador: MAJOR, TM Tiago Filipe Abreu Moura Guedes

Co-orientador: CAPITÃO-DE-FRAGATA, Sérgio R. Caldeira Carvalho

Pedrouços 2022

Declaração de compromisso antiplágio

Eu, **Bruno Manuel da Silva Pereira,** declaro por minha honra que o documento intitulado "**A evolução da relevância do Ciberespaço para a NATO"** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Estado-Maior Conjunto 2021/22** 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, 27 de junho de 2022

Assinado por : **Bruno Manuel da Silva Pereira**
Num. de Identificação: 12456592
Data: 2022.06.27 23:11:30+01'00'

Bruno Manuel da Silva Pereira

Agradecimentos

Dirijo as primeiras palavras de agradecimento ao meu orientador, o Major de Transmissões Tiago Filipe Abreu Moura Guedes, por toda a disponibilidade e apoio ao longo desta jornada. O profissionalismo e rigor que colocou na orientação, e revisão desta investigação permitiram atingir os objetivos propostos, pelo que ficarei para sempre grato. Uma palavra de agradecimento especial ao Capitão-de-fragata Caldeira Carvalho, por todo conhecimento e informação que partilhou, bem como por toda disponibilidade e camaradagem demonstrada.

Aos entrevistados, que, pela sua disponibilidade e franqueza permitiram desenvolver esta investigação, enriquecendo-a com os seus conhecimentos, sem o qual este estudo seria certamente mais pobre: Brigadeiro-general Viegas Nunes, Capitão-de-fragata Vasco Prates, Tenente-coronel Salomão Carvalho, Comandante Câmara da Assunção, Major Miguel Maria e ao senhor João Farinha. A todos vós, o meu muito obrigado.

Um agradecimento especial ao Coronel Quaresma Rosa, pela disponibilidade demonstrada desde o primeiro contacto, pelas diligencias efetuadas e por todo o conhecimento e experiência partilhada.

Ao Capitão-de-mar-e-guerra Fialho de Jesus, aquém agradeço pela disponibilidade e aconselhamento, mas sobretudo pelo conhecimento partilhado, o meu muito obrigado.

Um agradecimento ao Capitão-de-mar-e-guerra Carona Jimenez, diretor de curso, por todo auxílio concedido ao longo desta jornada e pela forma diligente como procurou apoiar o desenvolvimento dos trabalhos.

Aos meus camaradas de curso, em especial os que de mais perto me acompanharam, e que de diversas formas viabilizaram esta investigação, o meu muito obrigado.

Por último, aqueles que são o meu ponto de equilíbrio, e me inspiraram a ultrapassar as dificuldades, a minha esposa Andreia, e o meu filho António. À minha esposa Andreia, agradeço, por todo o apoio, compreensão e conhecimentos, sem o seu amor e generosidade esta tarefa não seria possível. Ao meu filho António, a quem peço desculpa pelos muitos momentos de ausência emocional, esperando no fim desta jornada poder compensar.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Índice de Tabelas

Resumo

Atualmente, o Ciberespaço é palco da proliferação de diversas ameaças, levando a *North Atlantic Treaty Organization* e os seus aliados a dedicar cada vez mais recursos que lhes permitam defender este domínio. Assim, com este estudo, pretendeu-se avaliar de que forma pode a Capacidade de Ciberdefesa nacional contribuir para o reforço da Capacidade de Ciberdefesa da *Aliança Atlântica.*

Adotou-se uma estratégia de investigação qualitativa, apoiada num raciocínio dedutivo. Como desenho de pesquisa utilizou-se estudo comparativo, num horizonte temporal transversal.

Na investigação realizada verifica-se que, o Ciberespaço, fruto das suas características e das ameaças, reveste-se de enorme importância para a *North Atlantic Treaty Organization,* materializando-se no seu reconhecimento como domínio das Operações Militares e na edificação da Capacidade de Ciberdefesa. Identificou-se que, neste domínio, a *Aliança Atlântica* possui vulnerabilidades nos vetores: Doutrina, Treino, Pessoal e Interoperabilidade, enquanto a capacidade portuguesa possui como potencialidades os vetores: Doutrina; Treino; Organização; e Interoperabilidade.

Conclui-se assim, que a Capacidade de Ciberdefesa das Forças Armadas portuguesas reúne potencial para reforçar a *Aliança* na produção de efeitos no Ciberespaço, enquadrada no mecanismo *Sovereign Cyber Effects Provided Voluntarily by Allies*, e no apoio à formação de pessoal especializado através da sua Escola de Ciberdefesa.

Palavras-chave: Ciberespaço; Operações Militares; Ciberdefesa; NATO; Forças Armadas portuguesas.

Abstract

Nowadays, Cyberspace is the scene of the proliferation of several threats, leading the North Atlantic Treaty Organization and its allies to dedicate more and more resources that allow them to defend themselves in this domain. Thus, this study was intended to assess how the national Cyber Defense Capability can contribute to the reinforcement of the North Atlantic Treaty Organization's Cyber Defense Capability.

A qualitative research strategy was adopted, supported by deductive reasoning, through a comparative study, as a research design, in a transversal time horizon.

In the investigation carried out, it appears that Cyberspace, as a result of its characteristics, and the implications for the conduct of military operations, is of enormous importance for the North Atlantic Treaty Organization, materialized in its recognition as a domain of military operations and the construction Cyberdefense capability. It is also concluded that the North Atlantic Treaty Organization's Cyberdefense capability has vulnerabilities in the following vectors: Doctrine, Training, Personnel, and Interoperability, while the Portuguese capability has the following vectors: Doctrine; Training; Organization; and Interoperability.

It is thus concluded that the Cyberdefense capability of the Portuguese Armed Forces has the potential to constitute itself as a reinforcement of the Cyberdefense capability of the Alliance in producing effects in Cyberspace, framed in the Sovereign Cyber Effects Provided Voluntarily by Allie's mechanism, and support for the training of specialized personnel through the Cyberdefense School.

Keywords: *Cyberspace; Military operations; Cyberdefense; NATO; Portuguese Armed Force*

Lista de abreviaturas, siglas e acrónimos

A

AJP	*Allied Joint Publication*

C

C2	Comando e Controlo
CCD	Centro de Ciberdefesa
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CCiber	Capacidade de Ciberdefesa
CCICE	Centro de Comunicações e Informação, Ciberespaço e Espaço
CCOM	Comando Conjunto para as Operações Militares
COCiber	Comando de Operações de Ciberdefesa
CWIX	*Coalition Warrior Interoperability Exploration, Experimentation, Examination Exercise*
CYOC	*Cyberspace Operations Centre*

D

DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade

E

ECD	Escola de Ciberdefesa
EMGFA	Estado-Maior-General das Forças Armadas
ExNCS	Exercício de Cibersegurança do Centro Nacional de Cibersegurança

F

FFAA	Forças Armadas

L

LOEMGFA	Lei Orgânica do Estado-Maior-General das Forças Armadas

M

MDN	Ministério da Defesa Nacional

N

NAC	*North Atlantic Council*
NATO	*North Atlantic Treaty Organization*
NCI*Academy*	*NATO Communications and Information Academy*
NCI*Agency*	*NATO Communications and Information Agency*
NCIRC	*NATO Computer Incident Response Capability*

O

ODC	Operações Defensivas no Ciberespaço
OE	Objetivo Específico
OG	Objetivo Geral
OOC	Operações Ofensivas no Ciberespaço

P

PDCCD	Plano de Desenvolvimento da Capacidade de Ciberdefesa
PDCM	Doutrina Militar Conjunta para Operações no Ciberespaço

Q

QC	Questão Central
QD	Questão Derivada

R

RCM	Resolução do Conselho de Ministros
RH	Recursos Humanos

S

SCEPVA	*Sovereign Cyber Effects Provided Voluntarily by Allies*
SHAPE	*Supreme Headquarters Allied Powers Europe*
SIC	Sistemas de Informações e Comunicações

T

TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação

1. Introdução

O Ciberespaço apresenta uma crescente importância para as sociedades, cada vez mais conectadas em rede, para os Estados que veem as suas infraestruturas críticas ameaçadas, e para as organizações, como é o caso da *North Atlantic Treaty Organization* (NATO), que necessitam de defender as suas redes de ameaças provocadas por atores estatais e não-estatais.

Assiste-se, nas últimas décadas, a uma crescente digitalização das sociedades, apoiada nos desenvolvimentos tecnológicos, potenciando o estreitar de relações, a criação de redes e consequentemente a globalização (Nunes, 2020, p.1). Como refere Jesus (2021), o Ciberespaço eliminou a barreira geográfica, pois a distância física e a barreira temporal imposta pelos diferentes fusos horários perderam relevância. Se o Ciberespaço oferece às sociedades modernas um conjunto diversificado de potencialidades, também as expõem a maiores riscos, e uma maior diversidade de ameaças. De acordo com Nunes (2018, p.81), numa sociedade em rede, as ameaças podem ter qualquer proveniência, e ter efeitos disruptivos e assimétricos, exponenciando os riscos sociais já existentes.

À semelhança do que acontece com a sociedade civil, também os desenvolvimentos tecnológicos tem tido uma forte influência nas Forças Armadas (FFAA) (Sigholm, 2016, p.22). De acordo com Nunes (2020, p.24) as operações militares estão cada vez mais dependentes das tecnologias de informação e comunicação (TIC) para garantirem o Comando e Controlo (C2), assim como os sistemas de armas estão cada vez mais dependentes das redes para operarem.

O Ciberespaço é atualmente explorado por ameaças estatais e não estatais, de natureza transnacional, expondo as vulnerabilidades civis e militares, obrigando a uma resposta integrada nos domínios civil-militar e nacional e internacional (Santos, 2018, p.33). Após o Ciberataque à Estónia em 2007, a NATO admitiu que o Ciberespaço seria palco de confrontação entre os Estados, tendo o conflito de 2008, entre a Rússia e a Geórgia demonstrado que os Ciberataques tinham o potencial necessário para se tornarem uma das componentes da guerra convencional (Maigre, 2022, p.4).

Face ao crescente número de ataques às suas redes, a NATO, ao longo das últimas duas décadas, tem dedicado cada vez mais atenção ao Ciberespaço, iniciando-se com o seu reconhecimento como o novo domínio das operações militares, e posteriormente com a extensão do Artigo 5º ao Ciberespaço (Brent, 2020, p.8). Concomitantemente, na Cimeira de Londres em 2019, os aliados assumiram o compromisso de aumentar as suas capacidades

de resposta a Ciberataques, de preparação, dissuasão e autodefesa, contra ameaças híbridas, que pretendam minar a segurança (Nunes, 2020).

Por sua vez, Portugal tem acompanhado a evolução do desenvolvimento da capacidade de Ciberdefesa (CCiber) da NATO, tendo-se iniciado em 2013, com a identificação das ameaças e o papel das FFAA na manutenção das infraestruturas nacionais no Conceito de Defesa Nacional (Ministério da Defesa Nacional [MDN], 2022). No início de 2022, fruto de alterações legais, a CCiber das FFAA portuguesas foi restruturada, encontrando-se este processo a decorrer.

Este trabalho de investigação tem como objeto de estudo as operações militares no Ciberespaço.

Tendo em consideração o objeto de estudo da investigação, a mesma será delimitada na esfera espacial e temporal (Santos et al., 2019). Ao nível espacial, este estudo será delimitado à NATO, e a Portugal, simultaneamente enquanto membro da NATO e possível contribuidor de capacidades para atuar no Ciberespaço. Por fim, na esfera temporal, será delimitado ao período compreendido entre os anos de 2002 e 2023, sendo o início deste coincidente com a primeira abordagem do ciberespaço numa cimeira da NATO, no ano de 2002, e o final coincidente com a data prevista para o término da edificação da CCiber das FFAA portuguesas.

O presente trabalho de investigação, tem o seguinte Objetivo Geral (OG):

OG: Avaliar de que forma pode a CCiber nacional contribuir para o reforço da capacidade da NATO para efetuar operações militares no Ciberespaço.

Assim, para que seja atingido o OG propõem-se os seguintes Objetivos Específicos (OE):

OE1: Analisar a relevância do Ciberespaço nas Operações Militares da NATO.

OE2: Analisar a CCiber da NATO.

OE3: Analisar a CCiber das FFAA portuguesas.

A melhor forma de iniciar uma investigação em Ciências Sociais é procurar enunciar o projeto sob a forma de pergunta de partida (Quivy & Campenhoudt, 2005). Desta forma, para responder ao OG deste estudo, formulou-se a seguinte QC:

QC: Em que medida pode a CCiber nacional contribuir para o reforço da capacidade da NATO para efetuar operações militares no Ciberespaço?

A partir do OG e respetivos OE, e atendendo à questão orientadora da pesquisa, foram elencadas as seguintes questões derivadas:

QD1: Em que medida o ciberespaço é relevante para as operações militares da NATO?

QD2: Que possibilidades e vulnerabilidades possui a CCiber da NATO?

QD3: Que possibilidades e vulnerabilidades possui a CCiber das FFAA portuguesas?

Este trabalho encontra-se organizado em cinco capítulos, iniciando-se com uma introdução ao tema. O segundo capítulo apresenta a revisão da literatura efetuada, definindo-se igualmente um conjunto de conceitos estruturantes que permitem uma melhor compreensão da problemática em estudo. O terceiro capítulo descreve a metodologia e método utilizado para a realização da investigação. Já o quarto capítulo visa apresentar os dados obtidos e efetuar a sua discussão, procurando responder às QD identificadas e consequentemente à QC. O quinto capítulo corresponde às conclusões, onde é refletido o percurso da investigação e as lacunas identificadas, além dos resultados obtidos, recomendações e propostas de estudos a efetuar.

2. Enquadramento teórico e conceptual

Este capítulo tem como objetivo apresentar o estado da arte e os conceitos estruturantes para esta investigação.

2.1. Revisão da Literatura

As operações militares no Ciberespaço tem sido alvo de diversos estudos ao longo do tempo. Destaca-se neste âmbito o estudo efetuado por Brantly e Smeets (2020), que motivados pelo reconhecimento público de diversos militares dos EUA da ausência de um pensamento doutrinal e conceptual no emprego das Capacidades militares no Ciberespaço, concluíram que o Ciberespaço está a ganhar cada vez mais importância económica, política e social, pelo que o emprego de operações militares no Ciberespaço irá continuar a ganhar preponderância nas próximas décadas.

Entendendo a importância que o Ciberespaço representa para os Estados, a NATO reconheceu na Cimeira de Varsóvia, em 2016, o Ciberespaço enquanto domínio das Operações militares. No seu estudo, Shea (2018), explora esta decisão da NATO, procurando determinar como a Aliança pode aumentar a sua capacidade de defesa e dissuasão através da edificação de Capacidades para atuar no Ciberespaço. Shea (2018) concluiu que o Ciberespaço é o ponto chave, que permitirá à NATO transitar de um paradigma de conflitos convencionais em grande escala, para um paradigma de conflito moderno assente em tecnologias do seculo XXI. O mesmo autor refere ainda que, o Ciberespaço permitirá à Aliança criar sinergias, através da produção de efeitos num domínio que poderão ter impacto noutro, aumentando a capacidade de defesa e dissuasão da NATO.

Se por um lado o Ciberespaço é um sem fim de possibilidades, também acarreta um conjunto de riscos e ameaças. Ablon et al. (2019), concluem que o Ciberespaço, enquanto domínio das operações militares está a evoluir muito rapidamente, fundamentalmente devido à tecnologia, mas também está a aumentar para os invasores, que o exploram, pelo que a NATO necessita de desenvolver esforços que lhe permitam antecipar efetivamente as intensões dos adversários e interromper as suas atividades, fornecendo em tempo oportuno capacidades para o combate.

Ao nível nacional relevam-se dois estudos envolvendo a temática das operações militares no Ciberespaço.

Pretendendo avaliar e identificar os efeitos através do reconhecimento do Ciberespaço pela NATO como domínio das operações militares para o Planeamento de Defesa Nacional, e para a edificação da CCiber, Honorato, Santos e Mateus (2017) concluíram que o Ciberespaço deveria passar a ser entendido como plataforma para o desenvolvimento de

operações, as quais as FFAA portuguesas deveriam ser capazes de atuar, dentro dos parâmetros, requisitos e procedimentos da NATO.

Nunes (2020), na sua investigação intitulada "A edificação da CCiber Nacional: Contributos para a definição de uma estratégia para o Ciberespaço", procurou analisar o impacto estratégico do Ciberespaço e definir uma estratégia militar para o Ciberespaço.

Para uma melhor compreensão do objeto de estudo, torna-se importante efetuar um enquadramento teórico e conceptual, nomeadamente: capacidade militar; Ciberespaço e Ciberdefesa.

2.1.1. Capacidades Militares

O palco de emprego de forças militares tem, ao longo do tempo, vindo a sofrer mutações, no último século os domínios do ar, espaço e ciberespaço juntaram-se aos domínios tradicionais terrestre e marítimo das operações militares (Caton, 2018, p.1). A NATO reconhece hoje quatro domínios de emprego das forças militares, o marítimo, o aéreo e espacial, o terrestre, e o Ciberespaço (NATO, 2020, p.5). De acordo com *Allied Joint Publication* (AJP) 3.20 (2020, p.1), a Aliança deverá possuir, à semelhança do que faz nos restantes domínios, a capacidade de se defender das ameaças, desenvolvendo para tal capacidades militares que lhe permitam atuar no Ciberespaço. Ao nível nacional, também as forças militares são organizadas em capacidades (Despacho n.º 11400/2014, de 11 de setembro), pelo que se torna importante entender o conceito de capacidade militar, sendo que não existe uma definição universal para este conceito.

Para a NATO (2021, p.23), uma Capacidade militar consiste na "capacidade de criar um efeito através do emprego de um conjunto de aspetos integrados, categorizados como: doutrina, organização, treino, material, desenvolvimento de liderança, pessoal, instalações e interoperabilidade".

Já a doutrina portuguesa refere a Capacidade militar como "o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para 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" (DOTMLPII[1]) (Despacho n.º 11400/2014, de 11 de setembro). Importa referir que, para esta investigação, o vetor Treino integra a componente formação, conforme Apêndice A.

[1] Ver Apêndice A – quadro conceptual

2.1.2. Ciberespaço

O Ciberespaço, constitui-se como um domínio para a condução de operações militares, podendo ser igualmente descrito como um campo de batalha não físico com uma componente física (Estado-Maior-General das Forças Armadas [EMGFA], 2022, p.3).

À semelhança do que sucede com o conceito anteriormente apresentado, não existe uma definição universal para o Ciberespaço.

Para a NATO, o Ciberespaço "[...] consiste em todas as comunicações interconectadas, as tecnologias de informação (TI), e outros sistemas tecnológicos, redes e os seus dados, incluindo os que são separados ou independentes, que processam, armazenam ou transmitem dados" (NATO, 2020a, p.4).

Já em Portugal, a Resolução do Conselho de Ministros (RCM) n.º 92/2019, de 5 de junho, que estabelece a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, define o Ciberespaço como "[…] ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

Tanto os Estados, como as organizações têm desenvolvido capacidades que lhes permitam defender as suas redes e o Ciberespaço.

2.1.3. Ciberdefesa

À semelhança do que acontece nos restantes domínios de atuação militar, o Ciberespaço é palco onde decorre, entre outras, operações militares. As Operações militares no Ciberespaço podem ser caracterizadas como "[…] atividades militares no, ou através do, ciberespaço que, delimitadas no tempo e no espaço e através da aplicação das capacidades de Ciberdefesa, se destinam a atingir os objetivos militares" (EMGFA, 2022, p.20).

Parece então revestir-se de importância a compreensão dos conceitos de Ciberdefesa, da NATO e de Portugal.

Assim, para a NATO, de acordo com o *Allied Joint Publication for Communications and Information Systems* (AJP-6) (2017, p.15),a Ciberdefesa é definida como: "[…] meio para alcançar e executar medidas para combater ataques cibernéticos e mitigar os seus efeitos, e assim preservar e restaurar a segurança da comunicação, informação e outros sistemas eletrónicos".

Por sua vez, Portugal define Ciberdefesa como "[…] uma atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço" (RCM n.º 92/2019, de 5 de junho).

2.2. Modelo de análise

Durante o percurso desta investigação foram identificados três conceitos estruturantes: o Ciberespaço, a Ciberdefesa e as capacidades militares. Para responder às QD, estes conceitos estruturantes foram analisados segundo as seguintes dimensões: O ciberespaço nas Operações militares; o Ciberespaço nas Operações militares da NATO, a CCiber da NATO; e a CCiber das FFAA portuguesas. A cada dimensão, associaram-se variáveis que permitiram estudar os conceitos de acordo com as QD. O Modelo de análise preconizado encontra-se refletido no Quadro 1.

Quadro 1 - Modelo de Análise

<table>
<tr><td>Tema</td><td colspan="5">A evolução da relevância do Ciberespaço para a NATO</td></tr>
<tr><td>Objetivo Geral</td><td colspan="5">Avaliar de que forma pode a Capacidade de Ciberdefesa Nacional contribuir para o reforço da capacidade da NATO para efetuar operações militares no Ciberespaço.</td></tr>
<tr><td>Questão Central</td><td colspan="5">Em que medida pode a Capacidade de Ciberdefesa Nacional contribuir para o reforço da capacidade da NATO para efetuar operações militares no Ciberespaço?</td></tr>
<tr><td>Objetivos Específicos</td><td>Questões Derivadas</td><td>Conceitos</td><td>Dimensões</td><td>Variáveis</td><td>Técnica de Recolha</td></tr>
<tr><td rowspan="5">OE1 – Analisar a relevância do Ciberespaço nas operações militares da NATO</td><td rowspan="5">QD1 – Em que medida o ciberespaço é relevante para as operações militares da NATO?</td><td rowspan="7">Ciberespaço;

Ciberdefesa;

Capacidades militares.</td><td rowspan="3">O Ciberespaço nas operações militares.</td><td>Características.</td><td rowspan="7">Análise documental / Entrevistas</td></tr>
<tr><td>Desafios e oportunidades.</td></tr>
<tr><td>Implicações.</td></tr>
<tr><td rowspan="2">O Ciberespaço nas Operações militares da NATO.</td><td>Relevância</td></tr>
<tr><td>Possibilidades e limitações.</td></tr>
<tr><td>OE2 – Analisar a capacidade de Ciberdefesa da NATO</td><td>QD2 - Que possibilidades e vulnerabilidades possui a capacidade de Ciberdefesa da NATO?</td><td>Capacidade de Ciberdefesa da NATO.</td><td>Possibilidades e limitações: DOTMLPII.</td></tr>
<tr><td>OE3 – Analisar a capacidade de Ciberdefesa das FFAA portuguesas</td><td>QD3 - Que possibilidades e vulnerabilidades possui a capacidade de Ciberdefesa das FFAA portuguesas?</td><td>Capacidade de Ciberdefesa das FFAA portuguesas.</td><td>Possibilidades e limitações: DOTMLPII.</td></tr>
</table>

O pensamento mental que enformou a presente investigação encontra-se materializado na Figura 1.

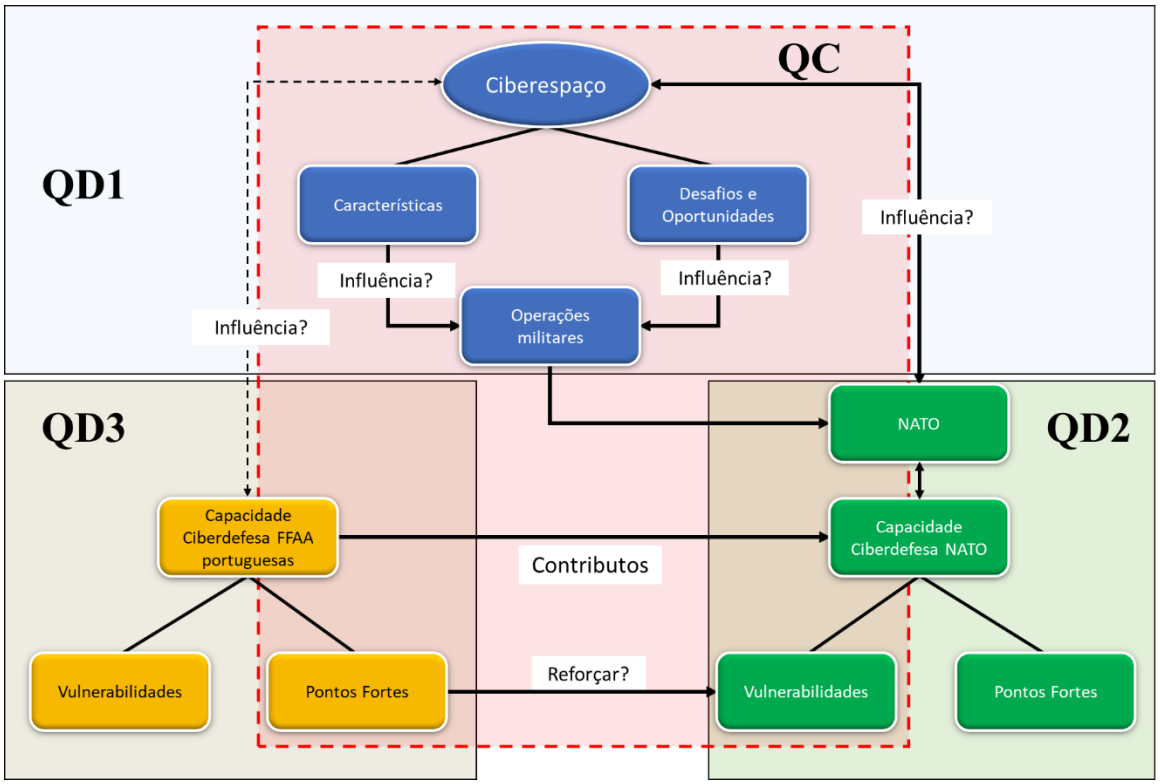

Figura 1 - Mapa mental da investigação

3. Metodologia e método

Pretende-se com o presente capítulo apresentar a metodologia e o método utilizado no desenvolvimento da investigação.

3.1. Metodologia

No sentido de atingir o OG proposto para esta investigação, utilizou-se o raciocínio dedutivo, partindo-se de uma lei geral para o particular a fim de obter conclusões (Santos et al., 2019), considerando que Portugal, enquanto membro, segue a doutrina da NATO.

A estratégia de investigação utilizada foi qualitativa, pretendendo-se recolher e analisar diferentes perspetivas por parte de especialistas, através de entrevistas e análise documental, permitindo ao investigador refletir sobre os mesmos para no final produzir conhecimento, não podendo ser analisadas através de métodos quantitativos. Na recolha de fontes documentais, procurou-se compreender as dinâmicas entre as operações militares e o Ciberespaço, assim como as CCiber da NATO e das FFAA portuguesas. Foram efetuadas entrevistas semiestruturadas, para compreender a relevância do Ciberespaço para a NATO, e quais as possibilidades e vulnerabilidades da CCiber da NATO e das FFAA portuguesas.

O desenho de pesquisa utilizado foi o estudo comparativo, com um horizonte temporal transversal, sendo o que melhor se adapta, tanto ao objeto de estudo, como ao tempo disponível, nomeadamente para a recolha das entrevistas. Este desenho de estudo incorporou a lógica da comparação, na medida em que podemos compreender melhor os fenómenos sociais quando são comparados (Bryman, 2012, p.72). Assim, comparam-se as possibilidades e limitações das CCiber da NATO e das FFAA portuguesas, com o objetivo de compreender de que forma poderá a CCiber nacional constituir-se como um reforço de capacidade para a NATO.

3.2. Método

3.2.1. Participantes e procedimento

A investigação do presente trabalho desenvolveu-se em duas fases distintas.

No decorrer da 1ª fase - exploratória, efetuou-se uma revisão da literatura, permitindo enquadrar o tema e conceitos estruturantes, identificar o objeto de estudo, o OG e respetivos OE. Esta fase, caracterizou-se pela análise documental de fontes primárias, que permitiram explorar os conceitos necessários para o enquadramento conceptual. Para complementar os conhecimentos adquiridos, foi realizada uma entrevista exploratória com o Chefe da Divisão de Planos do Centro de Ciberdefesa (CCD) do EMGFA.

A segunda fase – analítica/conclusiva, teve como objetivo responder às QD, através da análise dos dados recolhidos. O foco desta fase consistiu na recolha, análise e discussão

dos dados obtidos através da análise documental e das entrevistas realizadas, com o objetivo de validar as variáveis do modelo de análise, e identificar os indicadores[2] que permitiram retirar conclusões que materializam o OG. A análise documental foi efetuada com recurso à revisão da literatura, no sentido de aprofundar o conhecimento sobre o objeto de estudo. Foram efetuadas dez entrevistas, a especialistas nacionais e internacionais[3]. Ao nível nacional foram entrevistados especialistas, que desempenham ou desempenharam funções na área da Ciberdefesa, tanto na dependência do EMGFA como dos Ramos. Relativamente ao nível internacional, foram entrevistados especialistas que servem nas várias estruturas da NATO de Ciberdefesa, nomeadamente: *Cyber Defense Operations Centre* (CyOC), *NATO Communications and Information Academy* (*NCIAcademy*) e *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE).

3.2.2. Instrumentos de recolha de dados

Para as entrevistas foi elaborado um guião de entrevista constituído por onze questões[4]. Estas tiveram como principal objetivo obter informação não abordada pela bibliografia, nomeadamente as possibilidades e vulnerabilidades das CCiber da NATO e das FFAA portuguesas. Pretendeu-se ainda, confirmar a informação recolhida nos documentos analisados.

3.2.3. Técnicas de análise de dados

Para o tratamento dos dados obtidos nas entrevistas foi utilizada a aplicação informática *Nvivo* (1.6.1). A técnica de análise de dados utilizada foi a temática ou categorial (Guerra (2006) e Vilelas (2009), *cit.por* Santos et al., 2019, p.120).

Inicialmente efetuou-se uma análise de conteúdo sintetizadora, onde os contributos recolhidos foram agrupados e reunidos de forma similar, procurando-se uma redução do material pela condensação de afirmações (Flick, 2005, p.194).

Numa segunda fase, procurou-se uma análise do conteúdo estruturante, realizada ao nível formal, sendo classificados por unidade de significado, procurando-se obter uma compreensão mais profunda do texto (Flick, 2005, p.195).

Na apresentação dos dados, o *n* corresponde à amostra, representando o número de entrevistados que contribuíram para cada categoria. As referências correspondem à quantidade de vezes que surgem referências que contribuem para a mesma categoria ou subcategoria.

[2] Ver Apêndice F – Categorias e Subcategorias.
[3] Ver Apêndice D – Lista de entrevistados.
[4] Ver Apêndice C – Guião de entrevista.

4. Apresentação dos dados e discussão dos resultados

Por intermédio da análise documental e das entrevistas, procurou-se analisar o objeto de estudo em quatro dimensões: (i) O Ciberespaço nas Operações militares; (ii) O Ciberespaço nas operações militares da NATO; (iii) A CCiber da NATO; (iv) e a CCiber das FFAA portuguesas.

4.1. O Ciberespaço como domínio das Operações Militares da NATO

No presente subcapítulo serão apresentados os dados e discutidos os resultados das dimensões: O Ciberespaço nas Operações militares e o Ciberespaço nas Operações militares da NATO, sendo no final respondida a QD 1.

4.1.1. O Ciberespaço nas Operações Militares

Nas entrevistas realizadas, a variável "características do ciberespaço" teve contributos de 10 participantes, apresentando um total de 114 referências, podendo dividi-la em 19 subcategorias. As características mais apontadas foram: *"componente virtual"* (*n*=8 com 15 referências), *"componente física"* (*n*=7 com 10 referências), *"sem fronteiras"* (*n*=6 com 10 referências), "*tempo e velocidade*" (*n*=6 com 8 referências) e "*transversalidade*" (*n*=5 com 13 referências).

Segundo com o AJP 3.20 (2020, p.3), o Ciberespaço é composto por três camadas: a camada física, associada ao *hardware,* localizado numa área geográfica; a camada lógica, que consiste nos dados existentes, transformados em forma de código; e a camada *Ciberpessoa*, que consiste na representação virtual da pessoa, conforme Figura 2.

Figura 2 - Camadas do Ciberespaço
Fonte: Disponível em AJP 3.20 (2020, p.3).

A Publicação Doutrinária Militar Conjunta (PDMC) 3.20 (2022, p.3), refere que existe uma interdependência entre os domínios físicos, terra, mar, ar e espaço, uma vez que o Ciberespaço pode ser afetado por efeitos provocados nestes, mas pode-os também afetar através da criação de efeitos em cascata que conduzam à liberdade de ação para as operações

nos domínios físicos, conforme Figura 3. Esta transversalidade é igualmente destacada pelos entrevistados como relevante, e diferenciadora, e.g., *"Estou a falar a partir de um domínio atuar simultaneamente sobre todos os outros domínios, o que é absolutamente novo"* (Nunes, entrevista presencial, 30 de março de 2022).

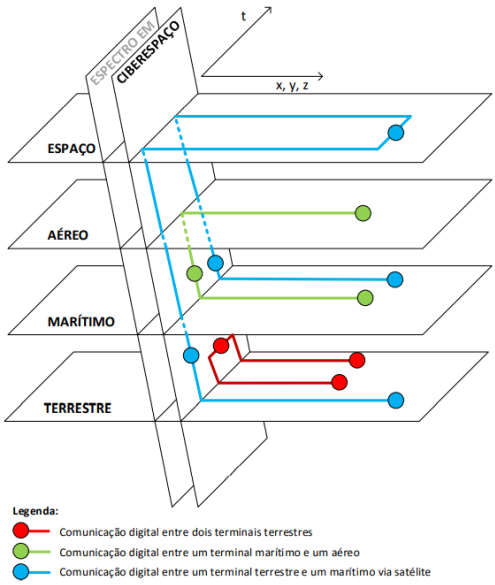

Figura 3 - Representação da relação do Ciberespaço com os restantes domínios
Fonte: Disponível em Honorato, Santos e Mateus (2017).

O AJP 3.20 (2020, pp. 13-14), apresenta o ciberespaço como um domínio que se diferencia dos restantes, por ser uma criação humana, parcialmente virtual, que não está delimitado por barreiras geográficas, o que também é referido pelos entrevistados, e.g., "*tem uma componente virtual, aquilo que é acedido através da componente física"* (Nunes, *op. cit.*), e.g., *"ausência do que possam ser consideradas fronteiras físicas"* (Assunção, entrevista por *email*, 07 de abril de 2022). Este domínio não se delimita geograficamente a uma área de operações, pelo que os seus efeitos não são limitados por barreiras ou limitações geográficas, e.g., "*As características que mais se releva do ciberespaço são o facto de se considerar que não possui fronteiras"* (Carvalho, entrevista via *Microsoft Teams*, 29 de março de 2022). Destaca-se ainda o tempo e velocidade, e.g., *"o triângulo Velocidade-Tempo-Alcance, que faz aumentar a surpresa de um ataque, reduzindo o intervalo de tempo que as organizações possuem para responder de forma adequada"* (Jesus, entrevista presencial, 23 de março de 2022).

Para além das características, os entrevistados referiram desafios e oportunidades apresentados pelo Ciberespaço.

A variável "Desafios e oportunidades**"** teve contributos de 10 participantes através de 82 referências, tendo sido dividida em "desafios" (com 13 subcategorias) e "oportunidades" (com 5 subcategorias).

Como desafios (*n*=10 e 54 referências), os entrevistados apontaram maioritariamente, a *"dependência*" (*n*=5 com 7 referências), a *"regulamentação"* (*n*=5 com 6 referências) e *as"ameaças" (n*=4 com 7 referências). As oportunidades que o ciberespaço apresenta (*n*=7 com 28 referencias) destaca-se a *"informação e conhecimento"* (*n*=4 com 10 referências) e a *"globalização"* (*n*=4 com 6 referências).

Um dos desafios referidos foi a elevada dependência do Ciberespaço, encontrando paralelismo com Nunes (2018, p.81), uma vez que a crescente dependência das sociedades modernas do Ciberespaço, em todas as dimensões da vida conduz ao aparecimento de vulnerabilidades e riscos, e.g., *"cria uma dependência extrema no ciberespaço"* (Farinha, entrevista por *email*, 06 de abril de 2022). Destaca-se igualmente a regulamentação como um desafio. Tal como refere Nunes (2020, p.103), o ciberespaço não possui espaços de soberania perfeitamente definidos, originando dificuldades de regulamentação, e potenciando o aumento de Ciberataques. Apesar disso, a NATO reconheceu que a lei internacional se aplica ao ciberespaço (AJP 3.20, 2020, p.19), tendo também Portugal incorporado na sua ordem jurídica estas orientações. Atribuiu-se igualmente relevância às ameaças enquanto desafios originados pelo Ciberespaço, e.g., *"A ausência de um entendimento à escala global sobre a governação e regulação da internet"* (Assunção, *op. cit.*). Como refere Nunes (2020, p.1), as vulnerabilidades do Ciberespaço podem ser exploradas por novas ameaças, muitas vezes de origem híbrida. Estas podem ser provenientes de atores estatais ou não estatais, possuindo diversas finalidades, desde o roubo até a ataques disruptivos (Jesus, 2021).

O Ciberespaço também potencia oportunidades, pois tal como refere Moniz (2018, p.17), permitiu a interação e acessibilidade veloz de informação e conhecimento. O Ciberespaço potencia a difusão de informação, e facilita o acesso ao conhecimento, o que se pode constituir com um fator de desenvolvimento das sociedades através do conhecimento, e.g., *"acessibilidade aos dados, à informação e ao conhecimento"* (Prates, entrevista via *Microsoft Teams*, 01 de abril de 2022). Uma outra oportunidade gerada pelo Ciberespaço corresponde à globalização, aproximando as pessoas de forma virtual, estreitou distâncias, criou redes aumentando os relacionamentos entre as pessoas (Nunes, 2020), e.g., *"na prática potencia a globalização"* (Carvalho, *op.cit.*).

Relativamente à variável "Implicações" do Ciberespaço para as operações militares, teve o contributo de todos os participantes (*n*=10), com 48 referências. Esta categoria foi dividida em 12 subcategorias, destacando-se *"impacto nos domínios tradicionais"* (*n*=5 com 13 referências) e *"comunicação e C2"* (*n*=5 com 9 referências).

O final do século XXI e início do presente século, assistiu a um rápido desenvolvimento das TI, bem como à disseminação generalizada da informação, originando uma mudança da natureza, métodos e técnicas utilizadas pelas FFAA (Steingartner & Galinec, 2021, pp. 28-29). Os conflitos militares modernos exigem cada vez mais conhecimento, e dependem de informação para gerar opções, fornecer informações e garantir o C2 das operações de combate (Hart & Klink, 2017, p.98). A importância da Comunicação e o do C2 para a condução das operações militares é igualmente referida pelos entrevistados, na medida em que, e.g., *"Qualquer sistema de comunicações ou de C2 depende do Ciberespaço"* (Farinha, *op. cit.*).

Esta crescente digitalização das forças militares, expõe-nas a maiores riscos de Ciberataques (Steingartner & Galinec, 2021, p.33). Como foi referido anteriormente, o Ciberespaço é um domínio transversal, sendo referido pelos entrevistados como tendo impacto significativo na condução das operações militares, pois a produção de um efeito num domínio poderá afetar os restantes, e.g., *"uma abordagem multi-domínio é absolutamente necessária"* (Anónimo, entrevista por *email*, 08 de abril de 2022). Por outro lado, devido à sua componente física, um efeito provocado num dos domínios tracionais, pode ter impacto no Ciberespaço. Assim, o futuro campo de batalha será um ambiente operacional *multi-domínio*, (Steingartner & Galinec, 2021, p.41).

4.1.2. O Ciberespaço nas Operações Militares da NATO

A dimensão "Operações militares no Ciberespaço da NATO", foi analisada de acordo com as seguintes variáveis: "Relevância "; e "Possibilidades e Limitações".

No que concerne à variável "Relevância", esta apresenta oito contributos com 32 referências, divididas em oito subcategorias, destacando-se a *"segurança"* (*n*=6 com 10 referências), e as *"novas capacidades"* (*n*=4 com 7 referências).

A NATO enfrenta um cenário mais exigente, complexo e em rápida evolução, o que exige uma maior capacidade de segurança. A dependência do ciberespaço, potenciado pelo carácter tecnológico do seu instrumento militar, assume-se como um desafio para a Aliança (NATO, 2018c, p.2). Esta necessita de estar capaz de defender as suas redes contra ameaças cada vez mais complexas, disruptivas e coercivas, e cada vez mais frequentes (NATO, 2022b), sendo esta necessidade reconhecida pelos entrevistados, e.g., *"reconhecimento da*

importância de garantir a segurança do ciberespaço, enquanto parte indissociável das operações militares atuais e futuras" (Farinha, *op. cit.*).

Procurado, responder aos desafios colocados pelas ameaças ao Ciberespaço, a NATO adotou desde 2002, na cimeira de Praga, diversas medidas que tem permitido atuar neste domínio, conforme Tabela 1. Para os entrevistados, a crescente relevância do Ciberespaço foi uma oportunidade para a NATO desenvolver novas capacidades que lhe permitisse defender as suas redes e consequentemente o Ciberespaço, e.g., *"oportunidade de desenvolver novas capacidades para operar no Ciberespaço"* (Farinha, *op. cit.*). Desta cimeira, segundo Jesus (2021), ficou estabelecido que a criação de efeitos no ciberespaço, ficaria a cargo dos seus aliados, através de um mecanismo denominado de *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA). Em 28 de fevereiro de 2018 foi emanada pela NATO a Visão e Estratégia militar para o Ciberespaço enquanto domínio das Operações (NATO, 2018c).

Tabela 1 - Evolução do Ciberespaço na NATO

CIMEIRA	PRINCIPAIS ATIVIDADES DESENVOLVIDAS PELA NATO
2002 – PRAGA *RECOGNISING*	Reconhecimento das Ciberameaças às redes da NATO
2008 - BUCARESTE *FOUNDING*	*Cyber Defence Policy 1.0.*
2010 - LISBOA *CENTRALISING*	A partir de 2010 a Ciberdefesa passou a constar no conceito estratégico da NATO *Cyber Defence Policy 2.0.* Adoção do Conceito Estratégico para o Ciberespaço
2014 - GALES *ENHANCING*	*Cyber Defence Policy 3.0.* Aplicação da Lei Internacional ao Ciberespaço Extensão do Artigo 5º
2016 - VARSÓVIA *ADAPTING*	Reconhecimento do Ciberespaço como um domínio das operações militares, no qual se deveria defender tal como no ar, no mar e na terra Foi ainda assumido o *Cyber Defense Pledge*, um compromisso que visa a melhoria da CCiber dos aliados como uma prioridade
2018 - BRUXELAS *OPERATING*	Acordo para criação de um CyOC, localizado na Bélgica, para garantir a compreensão situacional e coordenar as operações no ciberespaço
2021 - BRUXELAS	*Comprehensive Cyber Defence Policy*

Fonte: Adaptado de NATO (2022d).

Os entrevistados identificaram ainda possibilidades e limitações que o Ciberespaço pode colocar às operações militares da NATO.

Na categoria denominada "possibilidades e limitações" do Ciberespaço às Operações militares da NATO verificou-se um total de nove contributos com 24 referências. Subdivide-se esta em "possibilidades" (*n*=6 com 13 referências) e "limitações" (*n*=6 com 11 referências).

Na subcategoria "possibilidades" foram apontadas cinco subcategorias, sendo de referir o "conhecimento" (*n*=3 com 4 referências), e o "domínio operacional" (*n*=3 com 4 referências). No que respeita às limitações, esta dividiu-se em 8 subcategorias, destacando-se a "coordenação de operações" (*n*=2 com 2 referências).

A subcategoria "conhecimento" é referida pelos entrevistados considerando que através do Ciberespaço, a NATO tem a possibilidade de aumentar o seu conhecimento situacional relativamente aos seus adversários, e.g., *"podem permitir aumentar o conhecimento situacional sobre forças opositoras da Aliança Atlântica"* (Maria, *op. cit.*). Por sua vez, a categoria "domínio operacional" refere-se ao Ciberespaço como um domínio das operações militares, semelhante aos restantes, em que a Aliança deverá reunir todas a capacidades para conduzir operações. Como refere NATO (2018c, p.2), reconhece-se o Ciberespaço como um domínio das operações militares, que deve ser defendido à semelhança do que faz nos restantes, e.g., *"O sucesso operacional da NATO (…) encontra-se diretamente dependente da capacidade de estabelecer superioridade neste domínio operacional"* (Rosa, *op. cit*).

Os entrevistados referem, que a dependência do comandante operacional de outra entidade para produzir um efeito dificulta a coordenação das operações, nomeadamente na sincronização do efeito produzido no Ciberespaço, com a ação tática no domínio físico. Ao contrário do que sucede nos restantes domínios, a realização de Operações Ofensivas no Ciberespaço (OOC) é enquadrada no mecanismo SCEPVA, o que significa que a nação que produz o efeito fá-lo de forma independente, e a título nacional, não havendo uma integração NATO da produção deste, o que dificulta a sincronização das operações, e.g., *"a dificuldade na condução das operações uma vez que a criação de efeitos (SCEPVA) não está "debaixo" do Comandante Operacional, levando à necessidade de uma maior coordenação"* (Jesus, *op. cit.*).

4.1.3. Síntese Conclusiva

Da análise efetuada às características do Ciberespaço, em virtude de haver convergência entre a bibliografia e os contributos dos entrevistados, relevam-se como mais significativas as seguintes: (i) componente física e virtual; (ii) ausência de fronteiras; (iii) o tempo e velocidade; e (iv) a transversalidade. Identificou-se igualmente que o Ciberespaço apresenta desafios e oportunidades, que devem ser tidos em conta aquando da condução das operações militares, onde se realça como desafios: a elevada dependência do Ciberespaço; a necessidade de regulamentação; e a proliferação das ameaças. Já relativamente às oportunidades realça-se a facilidade de acesso à informação e conhecimento, e a

potencialização da globalização. Foi possível identificar um conjunto de implicações do Ciberespaço nas operações militares, sendo as mais relevantes: o impacto nos domínios tradicionais e o impacto na Comunicação e C2. Identificou-se igualmente que, o Ciberespaço é um domínio relevante para a condução das operações militares, realçando-se a importância de garantir a segurança e a geração de novas capacidades. Esta relevância materializa-se por diversas atividades desenvolvidas pela NATO, nomeadamente o reconhecimento do Ciberespaço como domínio das operações militares, a extensão do Art.º 5º, a difusão de políticas de defesa coletiva e a criação do CyOC. Identificaram-se, um conjunto de possibilidades e limitações que o Ciberespaço coloca às operações militares da NATO, sendo as mais relevantes: o acesso e disseminação de conhecimento e a criação de um novo domínio de atuação das forças militares. Relativamente às limitações, releva-se a impossibilidade de efetuar, de forma autónoma OOC, o que dificulta a coordenação das operações.

Assim, em resposta à QD1, conclui-se que o Ciberespaço enquanto domínio das operações militares, reúne um conjunto de características únicas, que o distingue dos restantes domínios tradicionais. Fruto destas características, o Ciberespaço oferece um conjunto de possibilidades, mas também de vulnerabilidades, podendo ter impacto nas operações militares, pelo que a NATO tem adotado diversas medidas que lhe permitam atuar neste domínio.

4.2. A Capacidade de Ciberdefesa da NATO

Neste subcapítulo são apresentados os dados referentes à análise documental e entrevistas realizadas relativamente à dimensão CCiber da NATO, bem como a discussão dos resultados. No final, é respondida a QD 2.

Em resultado das entrevistas realizadas, relativamente à categoria "A CCiber da NATO" (*n*=10 com 107 referências) foram identificados um conjunto de "possibilidades" (*n*=9 com 54 referências) e "vulnerabilidades" (*n*=10 com 56 referências).

Relativamente às "Possibilidades" e tendo em consideração os vetores de capacidade, a maioria dos entrevistados destacou a "Organização" (*n*=7 com 9 referências), seguindo-se a "Doutrina" (*n*=6 com 11 referências) e "Treino" (*n*=6 com 10 referências) como pontos fortes. Já relativamente às "vulnerabilidades", destacam-se os vetores "Doutrina" (*n*=8 com 19 referências), "Interoperabilidade" (*n*=7 com 14 referências), e "Pessoal" (*n*=6 com 9 referências).

No presente subcapítulo pretende-se apresentar de forma sucinta, a organização da CCiber da NATO, seguindo para tal os vetores de edificação de uma capacidade, DOTMLPII, assim como quais as suas possibilidades e vulnerabilidades.

O reconhecimento do Ciberespaço enquanto domínio das operações militares obrigou a NATO a desenvolver doutrina que permitisse, enquadrar este novo domínio (Marrone & Sabatino, 2021, p.8). Assim, em janeiro de 2020, foi publicada a AJP 3.20, com a finalidade de planear, executar e avaliar as operações do Ciberespaço no contexto das Operações Conjuntas (Maigre, 2022, p.5). Destaca-se ainda a elaboração da *Cyberspace Taxonomy and Terminology*, que permite enquadrar a tipologia de tarefas que podem ser desenvolvidas neste domínio, e fornecer a visão da Aliança para as operações no Ciberespaço, reforçando assim a interoperabilidade (NATO, 2018b, p.A-2). Doutrinariamente, segundo NATO (2018b, pp. A-2-A-7), esta desenvolve, de forma autónoma todo o tipo de operações no Ciberespaço, à exceção das OOC (Figura 4), tendo para tal desenvolvido um mecanismo denominado de SCEPVA[5], estabelecendo a criação de efeitos no ciberespaço, em apoio às operações militares da NATO, ficaria a cargo dos seus aliados (Jesus, 2021). Para os entrevistados, o vetor Doutrina é considerado um ponto forte, e um ponto fraco da CCiber da NATO. Ponto forte na perspetiva em que a doutrina aprovada pela NATO é consensual para os países aliados, facilitando a sua aceitação e integração, e.g., *"A doutrina que sai aprovada pela NATO é uma doutrina consensualizada entre os vários estados"* (Nunes, *op. cit.*). Em contraponto, é considerado uma vulnerabilidade para alguns dos entrevistados, sendo necessário alcançar consenso entre todos para a produção desta doutrina, e.g., "*Se por um lado a Doutrina pode ser um ponto forte na NATO, é também uma limitação, uma vez que qualquer alteração ou desenvolvimento de nova Doutrina tem de ser aprovada pelos 30 Aliados*" (Farinha, *op. cit.*), e os Estados com maior poder são os que influenciam a produção da doutrina, e.g., *"quem influencia a doutrina é quem tem mais força"* (Nunes, *op. cit.*).

[5] O mecanismo SCEPVA encontra-se discriminado no documento MCM-0151-2021, de 29 de setembro de 2021, contudo, devido ao seu grau de segurança ser reservado, não será abordado no presente trabalho.

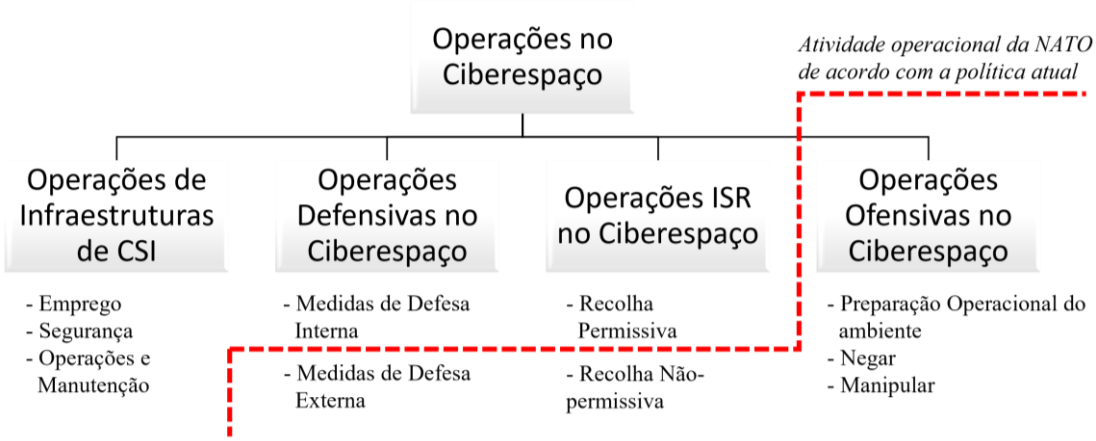

Figura 4 - Taxonomia das Operações no Ciberespaço
Fonte: Adaptado de NATO (2018b, p. A-1).

A NATO desenvolveu uma estrutura organizacional, que lhe permite, através do *North Atlantic Council* (NAC), exercer supervisão política de alto nível, em todos os aspetos relacionados com a implementação da política para o Ciberespaço, e exercer autoridade na gestão das crises relacionadas com a Ciberdefesa (NATO, 2022a), conforme Figura 5.

Ao nível político destacam-se o *Cyber Defense Commitee*, que se encontra subordinado ao NAC, tendo a responsabilidade de liderar a política de defesa do Ciberespaço da NATO (NATO, 2022a). Existe igualmente, o *Operations Planning Commitee*, desempenhando um papel de liderança no desenvolvimento e implementação de políticas relacionadas com as operações, e reforçando a colaboração entre os níveis político e militar (NATO, 2022c). Já ao nível militar, a Aliança conta com um CyOC, sediado em Mons na Bélgica, tendo como tarefas: promover de forma persistente e centralizada a compreensão situacional relativa ao Ciberespaço; promover no Ciberespaço todos os aspetos relacionados com a *Mission Assurance*; ser o ponto focal para a preparação, planeamento, conduta, coordenação e condução das Operações da NATO no Ciberespaço (NATO, 2022d, p.7). A Aliança conta também com a *NATO Communications and Information Agency* (NCI*Agency*), que tem como missão principal providenciar sistemas de informações e comunicações (SIC) à NATO (CCDCOE, 2022c). Este organismo possui na sua estrutura o *NATO Computer Incident Response Capability* (NCIRC), situado no *Supreme Headquarters Allied Powers Europe (SHAPE)* em Mons, na Bélgica, e tem como responsabilidade garantir a proteção técnica, de forma centralizada, dos sistemas da NATO (NATO, 2022b). Em apoio à NATO existe ainda o CCDCOE, que é o órgão acreditado pela NATO para a formação, aconselhamento, lições aprendidas, investigação e desenvolvimento no campo da Ciberdefesa (CCDCOE, 2022a). Os entrevistados referiram o vetor Organização como sendo

um ponto forte na perspetiva que o modelo organizativo da CCiber permite coordenar os esforços dos seus trinta membros para defenderem as redes da Aliança de forma integrada. Estes relevam ainda a importância do CyOC para a coordenação das atividades de Ciberdefesa e apoio às nações aliadas, e.g., *"uma estrutura capaz de coordenar a intervenção de apoios entre nações"* (Rosa, *op. cit.*).

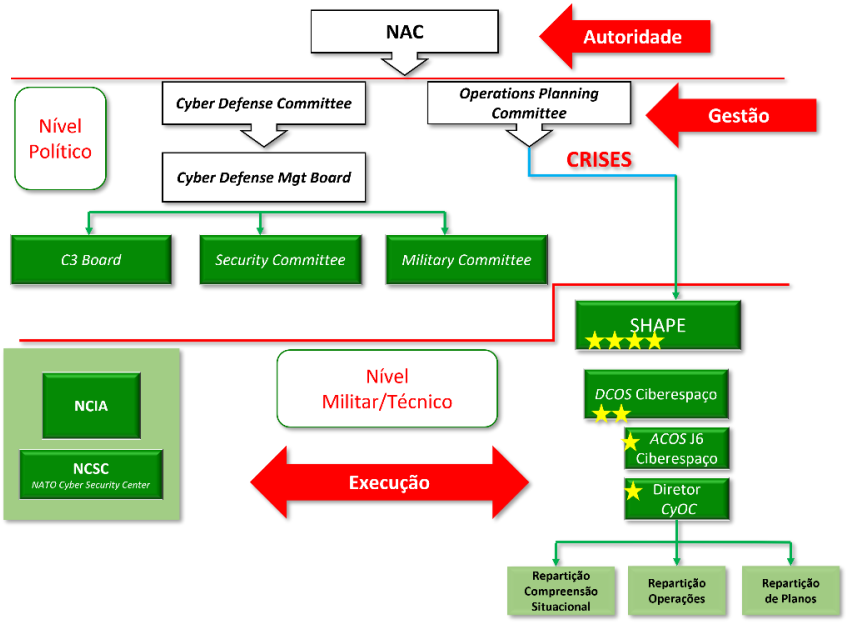

Figura 5 - Organização de Ciberdefesa da NATO
Fonte: Adaptado de NATO (2022d, pp.5-6).

Relativamente ao vetor Treino, onde se inclui a formação, é possível verificar que este ocorre aos vários níveis, Político, Estratégico, Operacional, Tático e Técnico, e por diversas entidades, conforme Figura 6.

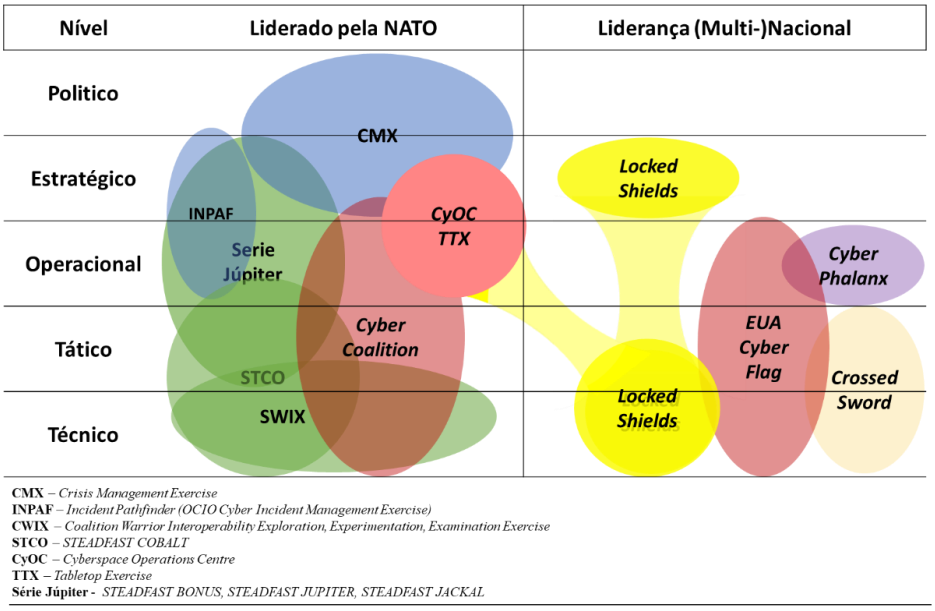

Figura 6 - Plano de treino do CyOC para o ano de 2022
Fonte: Adaptado de NATO (2022d, p.16).

De acordo com NCI*Agency* (2020, p.6) a NCI*Academy* é responsável pela oferta de serviços de formação e treino para a NATO e aliados, no que se refere à Ciberdefesa. As ações de formação da NCI*Academy* são orientadas para o desenvolvimento de competências técnicas (MDN, 2020, p.18), por outro lado, a *NATO School Oberammergau*, disponibiliza cursos de formação orientados para as operações de Ciberdefesa e o desenvolvimento procedimental da segurança das informações (MDN, 2020, p.18). De acordo com Marrone e Sabatino (2021, p.8), a NATO deveria aumentar o treino especializado dirigido a militares dedicados à Ciberdefesa. Por sua vez, os entrevistados referem o vetor Treino como ponto forte, na vertente dos exercícios, na medida em que promove diversos exercícios, que abrangem os diferentes níveis, desde o político ao técnico, e procuram promover a integração das capacidades nacionais dos países aliados, e.g., *"a NATO promove a realização periódica exercícios, designadamente o Cyber Coalition, bem como outros em parceria com o CCDCOE Tallinn, nomeadamente o Locked Shields e o Crossed Swords, que contam a participação de países da Aliança Atlântica e alguns países parceiros da NATO"* (Maria, *op. cit.*).

Relativamente ao vetor Material, e de acordo com Ďulík e Ďulík (2019, p.272), as redes militares são cada vez mais baseadas em tecnologias e protocolos de caris comercial que se encontram obsoletas. A NATO, encontra-se a desenvolver diversos programas de substituição dos equipamentos que constituem as suas redes, tendo em já em 2021, completado um projeto de substituição dos equipamentos do *NATO Cyber Security Centre* (NATO, 2022e).

Ao nível do vetor Liderança, verifica-se que existe uma visão integrada de todos os níveis de decisão (Figura 5). A visão da liderança política é materializada *SACEUR'S Direction and Guidance on Cyberdefense,* de 07 de abril de 2015, onde é estabelecida a orientação do SACEUR para o SHAPE e o *Allied Command Operations*, relativamente à estratégia de Ciberdefesa da NATO. Ao nível militar, o *Military Commitee*, materializa a sua visão para priorizar esforços no sentido de implementar o Ciberespaço enquanto domínio das Operações militares (NATO, 2018c).

A NATO reconhece na CCiber uma das suas prioridades, e para tal necessita de pessoal especializado, treinado a diferentes níveis (MDN, 2018, p.1). Para suprir a sua necessidade de pessoal qualificado para as suas estruturas, difunde ofertas de emprego públicas, às quais podem concorrer civis e militares, consoante os requisitos do cargo. Já no que se refere ao CCDCOE, é responsabilidade dos estados-membros a nomeação de pessoal especializado para as posições que lhes estão atribuídas (CCDCOE, 2022b). A escassez de RH qualificados

disponíveis para alimentar as estruturas de Ciberdefesa das Nações pode constituir-se um problema para a segurança nacional, e consequentemente para a NATO (Orye & Faith-Ell, 2020, p.3). Da perspetiva dos entrevistados, o vetor Pessoal é visto como uma vulnerabilidade da NATO, na medida em que existe uma escassez de pessoal com as qualificações necessárias para o desempenho de funções na área da Ciberdefesa *"As vulnerabilidades estarão sempre ligadas à existência de recursos humanos suficientes, e com as competências adequadas"* (Carvalho, entrevista por *email*, 04 de abril de 2022). Esta vulnerabilidade é ainda exponenciada pela dificuldade que os estes possuem em dotar a aliança com pessoal qualificado, pois são igualmente para si um recurso escasso *"Os países não prescindem dos seus recursos para disponibilizar à NATO porque estão totalmente dependentes deles para defender os seus sistemas"* (Carvalho, *op. cit.*).

A NATO possui infraestruturas em mais de 60 localizações diferentes, desde o Comando político em Bruxelas, até aos comandos militares nos diversos Teatros de Operações, o que significa que mais de 100.000 pessoas dependem da fiabilidade das suas redes (NATO, 2021b). No que se refere às infraestruturas orientadas para a Ciberdefesa, a NATO possui: Em Mons, na Bélgica, o CyOC, e no SHAPE o NCIRC; em Oeiras, em Portugal a NCI *Academy*; em Tallin, na Estónia o CCDCOE (NATO, 2021b).

A NATO procura reforçar a interoperabilidade com os seus aliados através da partilha de informação, troca de boas práticas e condução de exercícios para o desenvolvimento de especialistas (NATO, 2022a). A publicação doutrinária AJP 3.20, materializa, ao nível da doutrina o esforço para garantir a interoperabilidade com os seus aliados. Para desenvolver a sua interoperabilidade, e avaliar a sua CCiber, a Aliança conduz, conforme Figura 7, diversos exercícios. Existe ainda um esforço conjunto, entre a NATO e União Europeia no que se refere à troca de informação, ao treino, e à investigação e exercícios (NATO, 2022a). Marrone & Sabatino (2021, p.8), apontam três vulnerabilidades da NATO relativamente a este vetor, nomeadamente: ausência de uma estrutura de partilha com a EU para a regulação doutrinária; melhor integração do Ciberespaço nas estruturas de comando nacionais dos aliados; e reforço da colaboração, de forma estruturada e estratégica com empresas e entidades de investigação. Os contributos dos entrevistados referem igualmente este vetor como uma vulnerabilidade na perspetiva em que os países possuem muita relutância em partilhar o conhecimento relativamente à sua capacidade, e.g., *"A grande lacuna da NATO é interoperabilidade e partilha de conhecimento"* (Carvalho, *op. cit.*), e esta partilha torna-se ainda mais difícil quando se refere à condução das OOC, e.g., "*ninguém quer partilhar como produz os efeitos no Ciberespaço"* (Carvalho, *op. cit.*).

4.2.1. Síntese conclusiva

Conclui-se do presente subcapítulo, que a CCiber da NATO se encontra desenvolvida em todos os vetores de edificação, contudo foram identificados, tanto na análise documental, como pelo contributo dos entrevistados, pontos fortes e vulnerabilidades desta capacidade.

Em resposta à QD2, conclui-se que as principais potencialidades da CCiber da NATO relacionam-se com o vetor organização e Treino. Releva-se a organização, pela capacidade de coordenar os esforços de todos os seus membros, através do CyOC, e o Treino, na dimensão exercícios, pela sua abrangência, desde o nível político ao técnico. Já relativamente às vulnerabilidades, identifica-se ao nível doutrinário a inexistência de capacidade para desenvolver autonomamente OOC, dependendo da disponibilização voluntária dos aliados, bem como a necessidade de consensualização por todos os membros, e prevalência da doutrina do país mais poderoso. Também ao nível do treino identificam-se vulnerabilidades, na dimensão formação, devido à falta de formação especializada. Ao nível do pessoal, também existem vulnerabilidades, pela escassez de RH qualificados. Por fim, o vetor Interoperabilidade também se constitui uma vulnerabilidade, na medida em que não há partilha de conhecimento por parte dos seus membros, e identifica-se a necessidade de maior coordenação com a União Europeia, os países aliados e a indústria e investigação.

4.3. A Capacidade de Ciberdefesa das Forças Armadas portuguesas

No presente subcapítulo são apresentados os dados referentes à análise documental e entrevistas realizadas relativamente à dimensão CCiber das FFAA portuguesas, bem como a discussão dos resultados. No final, é respondida a QD 3.

Em resultado das entrevistas realizadas, relativamente à CCiber das FFAA portuguesas (*n*=10 com 102 referências), foram identificadas possibilidades (*n*=10 com 53 referências) e vulnerabilidades (*n*=9 com 49 referências) tendo como referência os vetores de capacidade.

Relativamente às "possibilidades" da CCiber nacional, os entrevistados destacam os vetores de capacidade *"treino"* (*n*=7 com 11 referências), *"organização"* (*n*=7 com 10 referências) e *"interoperabilidade"* (*n*=5 com 9 referências). Já no que concerne às "vulnerabilidades", destacam-se os vetores de capacidade *"pessoal"* (*n*=7 com 23 referências), *"treino"* (*n*=5 com 9 referências) e *"interoperabilidade"* (*n*=4 com 5 referências).

Para uma melhor compreensão da CCiber nacional, recorreu-se à metodologia DOTMLPII.

A produção de doutrina militar conjunta é da responsabilidade do Centro de Comunicações e Informação, Ciberespaço e Espaço (Decreto-Lei n.º 19/2022, de 24 de

janeiro). Até ao momento, foi submetida para aprovação, em março de 2022, a PDCM 3.20 (Carvalho, *op.cit.*). Esta publicação pretende criar as bases para a integração das CCiber dos Ramos das FFAA. Segundo a PDCM 3.20 (2022), as FFAA utilizam as suas capacidades no Ciberespaço para realizar Operações Defensivas no Ciberespaço (ODC) e OOC, conforme Figura 7 (PDCM 3.20, 2022, p.40).

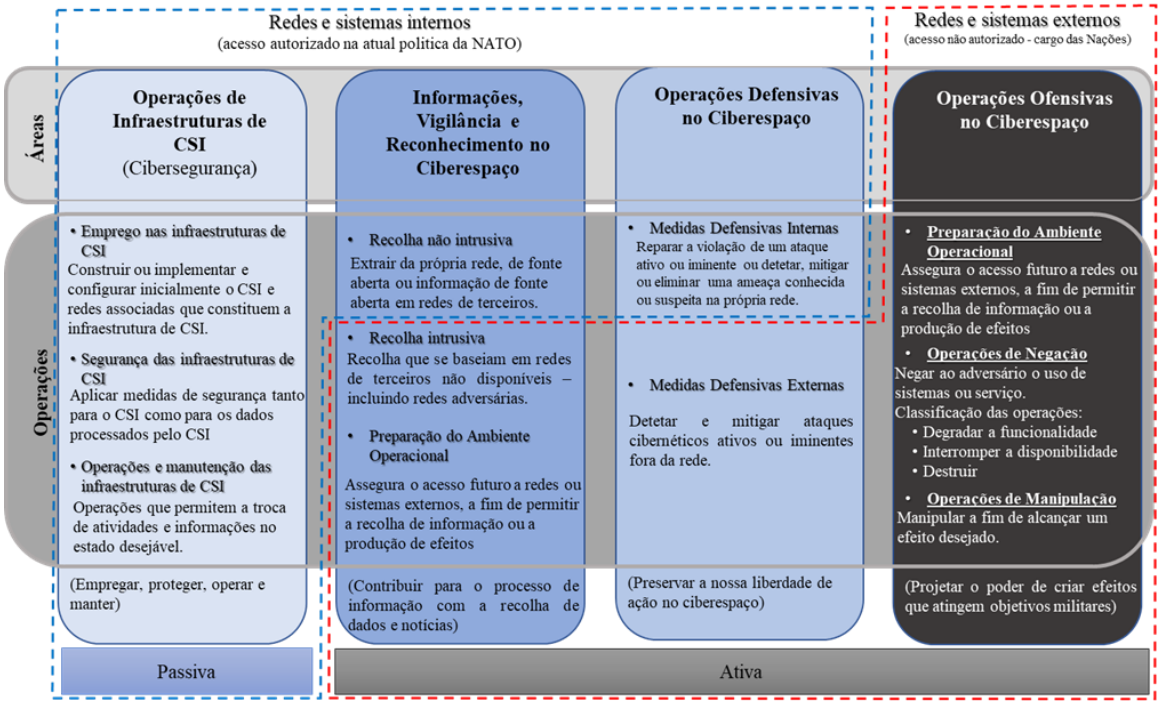

Figura 7 - Taxonomia das Operações no Ciberespaço
Fonte: Disponível em PDCM 3.20 (2022, p.25).

Ao nível da Organização, a estrutura de Ciberdefesa Nacional, fruto das recentes alterações legislativas, nomeadamente a Lei Orgânica do Estado-Maior-General das Forças Armadas (LOEMGFA), de 24 de janeiro, sofreu alterações significativas. Segundo a LOEMGFA, de 24 de janeiro, o EMGFA passa a contar com duas estruturas para a Ciberdefesa: O Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE); e o Comando de Operações de Ciberdefesa (COCiber). O CCICE tem como missão habilitar "a capacidade de C2 conjunto das FFFAA, assegurar o exercício do comando de operações militares no, e através do Ciberespaço, pelo Chefe do Estado-Maior-General das Forças Armadas, constituindo-se como o órgão de Ciberdefesa, e dirige os aspetos militares do programa espacial da defesa nacional" (Decreto-Lei n.º 19/2022, de 24 de janeiro). O CCICE compreende na sua estrutura a Escola de Ciberdefesa (ECD), que tem por missão "planear, dirigir, coordenar, controlar e executar operações no, e através do Ciberespaço em apoio a objetivos militares, garantindo a liberdade de ação das FFAA neste domínio" (Decreto-Lei n.º 19/2022, de 24 de janeiro 2022). O COCiber possui a seguinte estrutura: um Estado-

Maior; uma Força de Operações de Ciberdefesa; um Departamento de Sistemas de Ciberdefesa (Decreto-Lei n.º 19/2022, de 24 de janeiro 2022). De acordo com os entrevistados, a criação do COCiber irá contribuir para uma melhor articulação operacional, potenciando a coordenação entre o EMGFA e os Ramos, e.g., *"esta capacidade vai ser uma capacidade articulada com a componente operacional do EMGFA, do Comando Operacional do EMGFA, e o Comando do EMGFA tem em cada um dos ramos uma antena sobre a qual vai exercer comando"* (Nunes, *op. cit.*). Por outro lado, esta estrutura prevê a relação direta do COCiber com o Comando Conjunto para as Operações Militares (CCOM), o que aproxima o Ciberespaço dos restantes domínios das operações, e.g., "*a passagem do COCiber para a responsabilidade de coordenação do CCOM traduz o assumir do ciberespaço como um domínio de condução de operações e produção de efeitos"* (Rosa, *op. cit*.).

Ao nível do treino, a CCiber nacional participa em diversos exercícios, nacionais e internacionais. A nível nacional o CCD desenvolve e conduz o exercício *CyberDEx*, e participa no exercício de Cibersegurança do Centro Nacional de Cibersegurança (ExNCS), e no exercício promovido pelo Exército português, desde 2012, *Ciber Perseu* (MDN, 2022b). Ao nível internacional participa no *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise* (CWIX) (Nunes, 2020, p.48), no exercício da NATO *Cyber Coalition* e no exercício da CCDCOE *Locked Shields* (MDN, 2022b). De acordo com os contributos dos entrevistados, o vetor Treino, nomeadamente na vertente da formação, é considerado um ponto forte da CCiber nacional, na medida em que, através da ECD será possível formar os RH necessários com as competências necessárias, e.g., *"A criação da ECD, que permitirá garantir o treino individual necessários aos elementos que irão desempenhar funções no COCiber"* (Maria, *op. cit.*), permitindo validar as competências adquirida durante a formação. Segundo alguns entrevistados, o Treino, na dimensão dos exercícios, torna-se uma vulnerabilidade sendo que muitas vezes são colocadas restrições financeiras à sua realização, e.g., *"mas também o treino, que muitas vezes é condicionado pelas restrições financeiras associadas às necessidades de deslocamento e alojamento fora do país"* (Prates, *op. cit.*).

Relativamente ao vetor material, o Plano de Desenvolvimento da Capacidade de Ciberdefesa (PDCCD) 2021-2023 (2021, p.11), refere que deve ser garantida a evolução e sustentação das soluções tecnológicas da infraestrutura digital da Defesa Nacional. Para responder a este desígnio, a Lei de Programação Militar de 2019, prevê cerca de 45 milhões

de euros para a CCiber, num projeto de três quadriénios, de 2019 a 2030 (Lei Orgânica n.º 2/2019, de 17 de junho).

O COCiber relaciona-se diretamente com o CCOM e com o Centro de Informações e Segurança Militares, para efeitos de coordenação no âmbito do planeamento e da condução de operações militares no, e através do, Ciberespaço, conforme Figura 8 (EMGFA, 2021b, p.1).

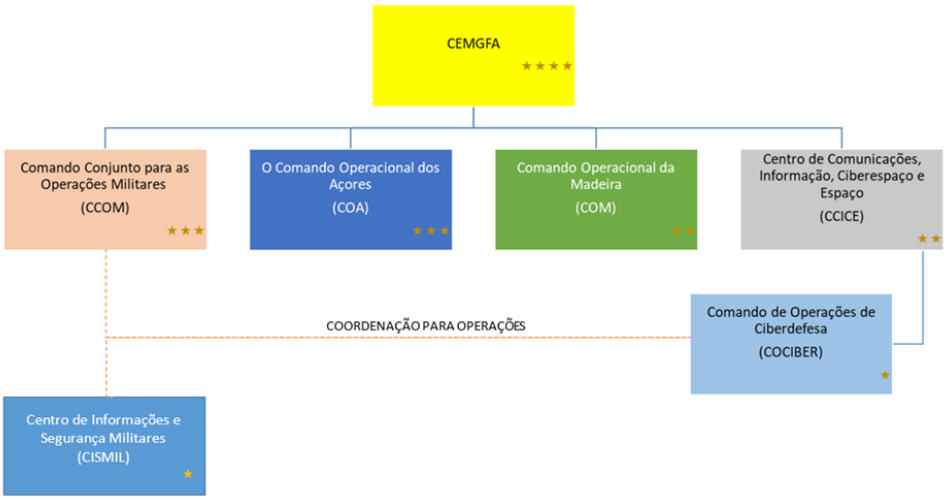

Figura 8 - Relações de Comando do COCiber
Fonte: Disponível em EMGFA (2021b, p.1).

Encontram-se ainda na dependência do COCiber o núcleo CIRC (NCIRC) do EMGFA e as componentes de Ciberdefesa dos Ramos, conforme figura 9 (EMGFA, 2021b, p.2).

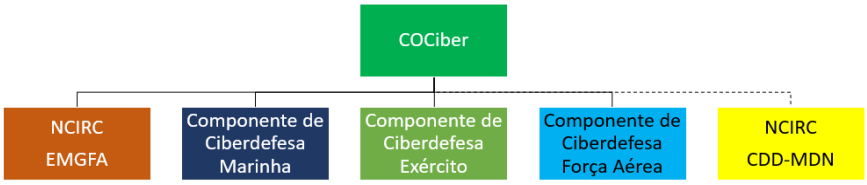

Figura 9 - Relações de dependência
Fonte: Disponível em EMGFA (2021b, p.1).

A Ciberdefesa é uma capacidade em desenvolvimento, verificando-se uma forte necessidade de aumento dos RH qualificados (MDN, 2020, p.4). A Direção-Geral dos Recurso Humanos da Defesa Nacional desenvolveu uma Política de RH para a Ciberdefesa, respondendo às necessidades de recrutamento, retenção e formação (MDN, 2020, p.1). De acordo com o PDCCD 2021-2023 (2021, p.35), a transformação do CCD em COCiber levará ao incremento de pessoal, passando de 90 militares para 250 militares e civis, e recrutados diretamente para a CCiber, contemplando os seguintes perfis profissionais: Ciberdefensor; Operações; Analista Forense; e Programador de Ciberdefesa. A estes números acresce ainda o efetivo necessário para a ECD e para as capacidades dos Ramos das FFAA (MDN, 2020,

p.4). O vetor "Pessoal" é referido pelos entrevistados como uma vulnerabilidade desta capacidade, considerando que existe uma escassez de recursos com qualificações necessárias para operar nesta área, e.g., *"a nossa principal vulnerabilidade neste estágio do desenvolvimento é o vetor do Pessoal"* (Assunção, *op. cit.*).

A atual CCiber, encontra-se sediada nas instalações do EMGFA, contudo, face à reformulação da CCiber está a sofrer, procura-se identificar as infraestruturas adequadas, nomeadamente para a ECD (EMGFA, 2021a, p.2).

No seu estudo, Nunes (2020, p.35), apontava o facto dos ramos das FFAA possuírem estruturas de Ciberdefesa diferentes, o que combinado com a ausência de doutrina e procedimentos técnicos consolidados dificultava a integração e articulação das capacidades residentes nos ramos. Com a difusão da PDCM 3.20, a lacuna doutrinária identificada por Nunes (2020) foi colmatada. Por outro lado, a restruturação da CCiber das FFAA, prevê que as componentes de Ciberdefesa dos Ramos passam a estar na dependência do COCiber (EMGFA, 2021b, p.2), o que deverá potenciar a interoperabilidade entre o EMGFA e os Ramos. Ainda no âmbito da interoperabilidade importa referir que o CCD participa no CWIX, que é o maior exercício da NATO no âmbito da Ciberdefesa, que visa permitir à NATO e aos seus aliados avaliar o nível de interoperabilidade da sua CCiber, e averiguar o nível de interoperabilidade dos seus sistemas de C2 para o cumprimento das suas missões (NATO, 2022b). Este vetor foi referenciado pelos entrevistados como um ponto forte, na medida em que, as componentes de Ciberdefesa dos Ramos encontram-se na dependência do COCiber, fomentando a interoperabilidade entre o EMGFA e os Ramos, e.g., "*a interoperabilidade era também um dos pontos fortes da capacidade de Ciberdefesa das nossas FFFAA"* (Prates, *op. cit.*). Por outro lado, a aquisição de material, para esta capacidade, é feita de forma centralizada no EMGFA, o que faz com que não haja diferentes equipamentos no EMGFA e no Ramos, e.g., *"Interoperabilidade porque ao ser o EMGFA a adquirir todos os equipamentos para as Forças Armadas, numa situação de compromisso entre todos e no desenvolvimento comum de requisitos, não existem sistemas diferentes para fazer o mesmo"* (Jesus, *op. cit.*). Os entrevistados referiram igualmente vulnerabilidades relativas a este vetor, sendo que se identifica que deveria haver maior cooperação interagências, por exemplo com a NATO e o Centro Nacional de Cibersegurança, e.g., *"deveria haver mais envolvimento Nacional com a NCIA"* (Prates, *op. cit.*).

4.3.1. Síntese conclusiva

Da análise anteriormente efetuada foram identificadas várias potencialidades e vulnerabilidades da CCiber nacional.

Assim, respondendo à QD3, identificam-se como principais potencialidades da CCiber das FFAA portuguesas, a Doutrina, o Treino, a Organização, e a Interoperabilidade, e como vulnerabilidades o vetor Pessoal. Considera-se que ao nível doutrinário assume relevância a possibilidade de efetuar toda a tipologia de Operações no Ciberespaço, sejam elas Defensivas ou Ofensivas, na medida em que, e.g., a NATO não possui essa capacidade.

Relativamente ao vetor Treino, este é considerado um ponto forte na dimensão da formação, nomeadamente pelas potencialidades geradas pela ECD, que se encontra em edificação, o que pode gerar sinergias na formação de pessoal especializado e na validação das suas competências. Já ao nível da Organização, a criação do COCiber assume igualmente grande relevância, permitindo uma maior integração operacional do Ciberespaço nas operações militares. E por fim, o vetor interoperabilidade, que através da ligação às capacidades dos Ramos, vai permitir uma maior interoperabilidade, constituindo um ponto forte da capacidade nacional.

Já como vulnerabilidades, foi identificado o vetor Pessoal, e assume grande relevância a escassez de pessoal qualificado para desenvolver funções nesta área.

4.4. Contributo para o reforço da Capacidade de Ciberdefesa da NATO

Neste capítulo procurou-se responder à QC, nomeadamente de que forma pode a CCiber das FFAA portuguesas contribuir para o reforço da CCiber da NATO.

Da análise efetuada verificou-se que o Ciberespaço, possui relevância para a NATO, tanto pelas suas características diferenciadoras, que fazem com que esta possa ter impacto na condução das operações militares, como pelas possibilidades e vulnerabilidades que pode originar às operações militares. Identificou-se igualmente que as principais vulnerabilidades CCiber da NATO são ao nível da Doutrina, materializada pela inexistência de capacidade para desenvolver autonomamente OOC, dependendo para tal da vontade dos aliados. Ainda ao nível doutrinário, a necessidade de consensualização por todos os membros, e prevalência da doutrina do país mais poderoso é vista como uma vulnerabilidade. Ao nível do treino, identificam-se vulnerabilidades, relacionadas com a dimensão formação, motivadas pela falta de formação especializada. Ao nível do pessoal, as vulnerabilidades materializam-se pela escassez de RH qualificados. Por fim, o vetor Interoperabilidade também se constitui uma vulnerabilidade, na medida em que não há partilha de conhecimento por parte dos seus membros, identificando-se a necessidade de maior coordenação com a União Europeia, os países aliados a indústria e investigação.

No que se refere às principais potencialidades da CCiber das FFAA portuguesas, identifica-se ao nível doutrinário a possibilidade de efetuar toda a tipologia de Operações no

Ciberespaço, Defensivas ou Ofensivas, ao contrário do que acontece com a NATO. Já ao nível do Treino, concretamente na dimensão da formação, identifica-se que pelas possibilidades geradas pela ECD em edificação, que poderão ser criadas sinergias na formação de pessoal especializado e na validação das suas competências. Ao nível da Organização, a criação do COCiber, vai permitir uma maior integração operacional do Ciberespaço nas operações militares, pelo que se constitui como um ponto forte. Por fim, o vetor Interoperabilidade, que através da ligação às capacidades dos Ramos, vai potenciar uma maior interoperabilidade.

Assim, em resposta à QC, conclui-se que a CCiber das FFAA portuguesas possui potencial para contribuir para o reforço da CCiber da NATO, através da produção de efeitos no Ciberespaço, e na formação de pessoal especializado. Enquadrado no mecanismo SCEPVA, Portugal poderá apoiar a NATO a colmatar a vulnerabilidade de não possuir autonomia para realizar OOC. A CCiber nacional pode ainda, reforçar a CCiber da NATO através da formação de pessoal especializado por intermédio da ECD. Este vetor assume grande relevância na medida em que pode criar sinergias entre Portugal e a NATO, através da ECD e da NCI*Academy*, não só na formação de pessoal qualificado, mas também no desenvolvimento de percursos formativos. De igual forma, poderá potenciar o desenvolvimento de competências de elementos nacionais que possam integrar a estrutura NATO, reforçando a atratividade para o recrutamento de pessoal para esta área de especialidade. As sinergias geradas neste vetor poderão tornar-se muito relevantes, não só para o reforço da capacidade, mas também para a sua sustentabilidade a médio e longo prazo, no que se refere aos RH qualificados.

Não se considera o vetor Interoperabilidade uma vez que esta apenas se identifica numa perspetiva interna da CCiber das FFAA portuguesas.

5. Conclusões

O Ciberespaço é atualmente explorado por diversas ameaças, o que obriga a uma constante resposta das organizações para defenderem as suas redes, como é o caso da NATO. Este estudo versou sobre a possibilidade de reforço da CCiber da NATO pela CCiber das FFAA portuguesas, tendo-se para tal identificado um conjunto de vulnerabilidades na CCiber da NATO, que a capacidade nacional reúne potencial para reforçar.

Para desenvolverem as suas atividades quotidianas, as sociedades dependem cada vez mais do Ciberespaço, fruto da proliferação das TI e dos sistemas em rede, que facilitam a troca de dados e o acesso à informação, tornando-se um elemento potenciador da globalização. Esta dependência não é exclusiva da sociedade civil, estende-se igualmente para a esfera militar, potenciada pela utilização das TIC e dos SIC nas forças militares. A sobrevivência, no moderno campo de batalha depende cada vez mais da obtenção de uma *Common Operational Picture* e da capacidade de C2 sobre as forças no terreno, tornando os exércitos mais avançados dependentes das suas redes, e, por conseguinte, do Ciberespaço. Esta dependência não é exclusiva dos SIC, ela verifica-se também nos sistemas de armas modernos, que operam cada vez mais em sistemas em rede. Se por um lado o Ciberespaço tem potenciado um sem fim de possibilidades, no ambiente civil e militar, este introduz também um novo fator na equação: novas tipologias de ameaças, as ciberameaças. O Ciberespaço tornou-se assim um local de proliferação constante de novas ameaças, estatais e não estatais, com motivações de largo espectro, desde motivação política até motivação pessoal. A NATO, enquanto organização tem sido alvo de um crescente interesse por estas ameaças, pelo que tem, ao longo das últimas décadas, adotado medidas que lhes permitam reforçar a segurança das suas redes, e dos seus aliados. Neste âmbito, importa referir o reconhecimento do Ciberespaço como domínio das operações militares, onde se aplicam as leis e convenções internacionais, e o artigo 5º da NATO. Por sua vez, Portugal, procurou acompanhar os desenvolvimentos da NATO, edificando a sua CCiber, sendo a mesma materializada pela criação do CCD em 2015. A importância desta capacidade é patente na restruturação que se encontra a ser efetuada, no âmbito da revisão da LOEMGFA de 24 de janeiro de 2022.

Para a realização da presente investigação foi empregue o raciocínio dedutivo. Para tal foi utilizada uma estratégia qualitativa, que permitiu extrair conclusões relativamente aos dados recolhidos.

Foram efetuadas dez entrevistas a especialistas nacionais, e internacionais no âmbito da Ciberdefesa. A nível nacional, os entrevistados desempenhavam funções no MDN,

EMGFA e nos três Ramos das FFAA, tendo desempenhado previamente funções na área da Ciberdefesa. No que se refere aos entrevistados internacionais, desempenham funções em várias estruturas da NATO, nomeadamente: CyOC, NCI*Academy* e CCDCOE.

O Ciberespaço enquanto domínio das operações militares, reúne um conjunto de características únicas que o distingue dos restantes domínios tradicionais. Fruto destas características, o Ciberespaço oferece um conjunto de potencialidades, mas também de vulnerabilidades, pelo que pode impactar na condução das operações militares da NATO. Verificou-se igualmente que a NATO atribuiu extrema relevância ao domínio do Ciberespaço, nomeadamente no seu reconhecimento como um domínio das operações militares, e na edificação de uma capacidade própria para atuar no Ciberespaço. Esta capacidade encontra-se desenvolvida em todos os vetores de edificação, contudo, apurou-se, através do contributo dos entrevistados, um conjunto de vulnerabilidades, nomeadamente nos vetores: Doutrina, Treino, Pessoal e Interoperabilidade. Observou-se ainda que, as principais potencialidades identificadas na CCiber das FFAA portuguesas são nos vetores: Doutrina; Treino; Organização; e Interoperabilidade. Já como principais vulnerabilidades da CCiber nacional foi identificado o vetor Pessoal.

Conclui-se que a CCiber das FFAA portuguesas possuem potencial para se constituírem como um reforço da CCiber da NATO nos vetores: Doutrina e Treino. Uma das possibilidades da capacidade nacional materializa-se através da produção de efeitos no Ciberespaço, pelo que, enquadrada no mecanismo SCEPVA permite colmatar a vulnerabilidade da NATO nesta tipologia de operação. A CCiber nacional pode ainda, reforçar a CCiber da NATO através do vetor Treino, nomeadamente apoiando a formação de pessoal especializado por intermédio da ECD, que se encontra em edificação.

Tendo em considerando a investigação realizada, e atendendo aos resultados alcançados, realçam-se os contributos considerados como mais relevantes para o conhecimento. Em primeiro lugar destacar o Ciberespaço enquanto domínio das operações, que face às suas características únicas, potencia a condução das operações militares, mas também pode provocar vulnerabilidade, o que pode impactar na condução das operações militares conduzidas pela NATO. Em segundo lugar, foram identificadas as potencialidades e vulnerabilidades das capacidades de Ciberdefesa da NATO e das FFAA portuguesas, o que permitiu identificar a criação de possíveis sinergias entre estas entidades, de forma a explorar os pontos fortes e a mitigar as vulnerabilidades, tornando a defesa das redes da NATO e de Portugal mais resilientes.

Durante a condução da presente investigação foram identificadas limitações à mesma. Realça-se como primeira limitação o grau de segurança da maioria dos documentos de referência, de origem NATO, o que impossibilitou a utilização do seu conteúdo numa investigação que se pretende ser de fonte aberta. O objeto de estudo possui um carácter sensível, nomeadamente a identificação de vulnerabilidades, o que condicionou o contributo de alguns entrevistados, especialmente os internacionais. Outra limitação vivenciada prende-se com a disponibilidades de especialistas para entrevistar, que ao nível nacional são reduzidos. Por fim, e no seguimento desta limitação anteriormente referida, não foi adequado entrevistar o Exmo. Chefe do CCD em virtude de este ter sido nomeado arguente da defesa da presente investigação.

Face às conclusões obtidas com o presente estudo, nomeadamente no que se refere à capacidade identificada no vetor Treino, propõe-se que seja estudado um modelo de cooperação entre a ECD das FFAA portuguesas e a NATO, no sentido de mitigar a escassez de RH, e validar as suas competências.

Referências Bibliográficas

Ablon, L., Senty, D., & Thompson, J. (2019). *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*. Santa Mónica: RAND Corporation.

Brantly, A., & Smeets, M. (2020). Military Operations in Cyberspace. Em: A. Sookermany (Ed.), *Handbook of Military Sciences* (pp. 1–16). Cham: Springer International Publishing.

Brent, L. (2020). *The Past, present and future of NATO's Cyber Defence, 1(36)*. Pp. 1–12. Retirado de https://jwc.nato.int/application/files/2716/0523/5513/issue36_02lr.pdf

Bryman, A. (2012). *Social Research Methods* (4.ª Ed.). Nova Iorque: Oxford University Press.

Caton, J. (2018). *The Land, Space, and Cyberspace nexus: Evolution of the oldest military operations in the newest military domains*. Carlisle: *US Army War College*.

Decreto-Lei n.º 19/2022, de 24 de janeiro. (2022). *Lei Orgânica do Estado-Maior-General das Forças Armadas*. Diário da República, 1.ª Série, 16, 3-97. Lisboa: Presidência do Conselho de Ministros.

Ďulík, M., & Ďulík, M. (2019). Cyber security challenges in future military battlefield information networks. *Advances in Military Technology*, *14*(2), pp. 263–277. Doi: 10.3849/aimt.01248

Estado-Maior-General das Forças Armadas (2021a). *Plano de Desenvolvimento da Capacidade de Ciberdefesa 2021-2023*. Lisboa: Autor.

Estado-Maior-General das Forças Armadas (2021b). *Regulamento Interno do Comando de Operações de Ciberdefesa*. Lisboa: Autor.

Estado-Maior-General das Forças Armadas. (2022). *PDMC 3.20 Doutrina Militar Conjunta para Operações no Ciberespaço*. Lisboa: Autor.

Flick, U. (2005). *Métodos Qualitativos na Investigação Científica*. Lisboa: Monitor, Lda.

Hart, W., & Klink, M. (2017). *1st Troll Battalion: Influencing Military and Strategic Operations through Cyber-Personas*. *Paper* apresentado na *2017 International Conference on Cyber Conflict (CyCon U.S.)*. Washington, DC.

Honorato, M., Santos, L., & Mateus, R. (2017). *O Ciberespaço como 5.º Domínio Operacional. Impacto estratégico na Política de Defesa Nacional*. Trabalho de Investigação de Grupo do curso de promoção a Oficial General). Instituto Universitário Militar, Lisboa.

Jesus, F. (2021). Ciberdefesa - Uma Componente de Cibersegurança. *Revista Militar, 2631.* Retirado de https://www.revistamilitar.pt/artigo/1545.

Lei Orgânica n.º 2/2019, de 17 de junho (2019). *Lei de Programação Militar*. Diário da República, 1.ª série, 114, 2982 a 2985. Lisboa: Assembleia da República.

Maigre, M. (2022). *NATO's Role in Global Cyber Security*. Washington, DC: The German Marshall Fund of the United States

Marrone, A., & Sabatino, E. (2021). *Cyber defence in NATO countries: comparing models*. Roma: Istituto Affari Internazionali

Despacho n.º 11400/2014, de 11 de setembro. (2014). *Diretiva Ministerial de Planeamento de Defesa Militar*. *Diária da República*, 2ª série, 175. 23656 a 23657. Lisboa: Ministério da Defesa Nacional.

Ministério da Defesa Nacional. (2018, abril). "NATO-EU Cooperative Cyber Defence Capability Building" How Smart Defence and Pooling & Sharing can foster Cooperation, Transformation and Innovation. Em: Ministério da Defesa Nacional, *CD SDP Cyber Defence Smart Defence Projects.* Simpósio organizado pelo Ministério da defesa Nacional, Lisboa.

Ministério da Defesa Nacional. (2020). *Política de Recursos Humanos para a Ciberdefesa*. Lisboa: Autor.

Ministério da Defesa Nacional. (2022ª, 30 de abril). *Enquadramento da Ciberdefesa* [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/enquadramento/Paginas/default.aspx

Ministério da Defesa Nacional. (2022b, 30 de abril). *Exercícios de Ciberdefesa* [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios

NATO Cooperative Cyber Defence Centre of Excellence. (2022a, 30 de abril). *About us* [Página *online*]. Retirado de https://ccdcoe.org/about-us/

NATO Cooperative Cyber Defence Centre of Excellence. (2022b, 30 de abril). *Careers* [Página *online*]. Retirado de https://ccdcoe.org/careers/

NATO Cooperative Cyber Defence Centre of Excellence. (2022c, 30 de abril). *North Atlantic Treaty Organisation* [Página *online*]. Retirado de https://ccdcoe.org/organisations/nato/

NATO Communications and Information Agency. (2020). *NCI Academy: C4ISR & Cyber Training Catalogue - 2021*. (5.1). Bruxelas: Autor.

North Atlantic Treaty Organization. (2015). *SACEUR'S Direction and Guidance on Cyber Defence*. Bruxelas: Autor.

AJP-6. (2017). *Allied Joint Publication for Communications and Information Systems*. Bruxelas: NATO Standardization Office.

AAP-06. (2021). *Glossary of Terms and Definitions*. Bruxelas: NATO Standardization Office.

AJP-3.20 (2020a). *Allied Joint Doctrine for Cyberspace Operations*. Bruxelas: NATO Standardization Office (NSO).

North Atlantic Treaty Organization. (2022a, 22 de março). *Cyber defense*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

North Atlantic Treaty Organization. (2018b). *High Level Taxonomy of Cyberspace Operations*. Norfolk: Autor.

North Atlantic Treaty Organization. (2021b, 22 de março). *NATO Cyber Defence* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

North Atlantic Treaty Organization. (2022b, 30 de abril). *Federated Interoperability* [Página *online*]. Retirado de https://www.act.nato.int/federated-interoperability

North Atlantic Treaty Organization. (2018c). *Military Vision and Strategy on Cyberspace as a Domain of Operations*. Norfolk: Autor.

North Atlantic Treaty Organization. (2022c, 28 de março). *Operations Policy Committee* [Página *online*]. Retirado de https://www.nato.int/cps/en/natolive/topics_69312.htm

North Atlantic Treaty Organization. (2022d, 28 de março). *NATO's perspective on Cyberspace Operations-CyOC*. Cyberspace Operations Centre [Página *online*]. Retirado de https://www.nato.int/cps/en/natolive/topics_69312.htm

North Atlantic Treaty Organization. (2022e, 9 de fevereiro). *NATO refreshes cyber security technology to protect its networks* [Página *online*]. Retirado de https://www.ncia.nato.int/about-us/newsroom/nato-refreshes-cyber-security-technology-to-protect-its-networks.html

Nunes, P. F. V. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço*. Coleção "ARES", 36. Lisboa: Instituto Universitário Militar.

Nunes, P., Moniz, P., & Casimiro, S. (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: Idn cadernos.

Orye, E., & Faith-Ell, G. (2020). *Cyber workforce recruitment and retention: an awareness*. Tallin: CCDCOE.

Quivy, R., & Campenhoudt, L. van. (2005). *Manual de investigação em ciências sociais* (4.ª Ed.). Lisboa: Gradiva.

Resolução do Conselho de Ministros n.º 92/2019. (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1.ª série. 108. pp. 2888–2895. Lisboa. Resolução do Conselho de Ministros.

Santos, L., & Lima, J. (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação* (2.ª Ed.). Cadernos do IUM, 8. Lisboa: IUM.

Shea, J. (2018). Cyberspace as a Domain of Operations: What Is NATO's Vision and Strategy? *MCU Journal,* 9(2), pp. 133-150. doi: 10.21140/mcuj.2018090208

Sigholm, J. (2016). *Secure Tactical Communications for Inter-organizational Collaboration: The Role of Emerging Information and Communications Technology, Privacy Issues, and Cyber Threats on the Digital Battlefield* (Tese de Dissertação de Doutoramento). University of Skövde, Skövde.

Steingartner, W., & Galinec, D. (2021). Cyber Threats and Cyber Deception in Hybrid Warfare. *Acta Polytechnica Hungarica*, *18*(3), pp. 25-42. Retirado de http://acta.uni-obuda.hu/Steingartner_Galinec_110.pdf

Apêndice A — Quadro de Conceitos

Ciberataque – Ataque realizado através das tecnologias de informação no ciberespaço dirigido contra um ou vários sistemas, com o objetivo de prejudicar a segurança das tecnologias de informação e da comunicação (confidencialidade, integridade e disponibilidade), em parte ou totalmente (CNCS, 2022).

Cibersegurança - 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 e disponibilidade da informação, das redes digitais e dos sistemas de informação no ciberespaço, e das pessoas que nele interagem (CNCS, 2022).

Comando e Controlo – autoridade, responsabilidade e atividade dos Comandantes militares na direção e coordenação das forças militares, assim como na implementação de ordens relacionadas com as operações (NATO, 2021, p.29).

Desinformação – criação e disseminação deliberada de informação falsa ou manipulada com a intenção de enganar (NATO, 2020).

Doutrina – representa um pensamento comum (maneira comum de pensar) ou uma boa prática para uma situação específica ou problema. A Doutrina engloba táticas e procedimentos específicos para a condução/ execução de tarefas (EMGFA, 2021, p. A-3).

Educação (formação) e Treino – inclui o espectro total de formação, treino individual e coletivo e exercícios (EMGFA, 2021, p. A-3).

Infraestruturas – termo para todas as infraestruturas/ instalações necessárias para acomodar, treinar e preparar uma força militar (EMGFA, 2021, p. A-3).

Interoperabilidade – refere-se á capacidade se poder ligar ao mundo externo e interagir com outras capacidades. Inclui entre outros os domínios tecnológico, doutrinário e cultural (EMGFA, 2021, p. A-3).

Liderança – refere-se a como as chefias militares devem utilizar uma determinada capacidade. Por exemplo utilizar forças especiais para tarefas de infantaria não faz sentido (EMGFA, 2021, p. A-3).

Material – o hardware (HW) e software (SW), inclui equipamento específico, sistemas de armas, sobresselentes e tecnologias (EMGFA, 2021, p. A-3).

Organização – define a estrutura e agrupamentos que são utilizados (EMGFA, 2021, p. A-3).

Operações Defensivas no Ciberespaço – são operações executadas para preservar e/ou restaurar a capacidade de utilizar o ciberespaço de interesse nacional e proteger os dados, redes, sistemas de informação e outros sistemas da RDN, ou outra área do ciberespaço onde as FFAA tenham sido mobilizadas para a defesa contra ameaças ativas no ciberespaço (EMGFA, 2022, p.22).

Operações no Ciberespaço – ações no ou através do ciberespaço destinadas a preservar a liberdade de ação amigável em ciberespaço e/ou para criar efeitos para atingir os objetivos dos comandantes (AJP 3.20, 2020, p.4).

Operações Ofensivas no Ciberespaço – são missões das OpsCiber destinadas a projetar poder no, e através do, ciberespaço exterior por intermédio de ações realizadas para apoiar os Comandos Operacionais e os Comandos de Força-tarefa ou para atingir os objetivos militares (EMGFA, 2022, p.24).

Pessoal – representa o tipo/ quantidade de militares que são precisos. Dever-se-á incluir a identificação de especialistas e/ ou as competências necessárias (EMGFA, 2021, p. A-3).

Tecnologias disruptivas – Uma tecnologia que teve, ou espera-se que tenha um efeito revolucionário no setor da Defesa/Segurança, e/ou nas funções das empresas (NATO, 2021, p.43).

Apêndice B — Relação entre Questões derivadas e Questões das entrevistas

Quadro 2 - Relação entre Questões Derivadas e Questões das entrevistas

Questão Derivada	Pergunta da entrevista
QD1 - Em que medida o ciberespaço é relevante para as operações militares da NATO?	1.1. Tendo em consideração a sua experiência nesta área, quais as características que destacaria do Ciberespaço? 1.2. Na sua visão, quais considera serem os desafios e oportunidades mais relevantes que o Ciberespaço apresenta para as pessoas, organizações e sociedades? 1.3. De acordo com a sua perspetiva quais as principais implicações que o Ciberespaço apresenta às Operações militares? 2.1. No seu entender quais as principais razões que levaram a NATO a reconhecer o Ciberespaço enquanto domínio das Operações militares, independente do terrestre, naval, aéreo e espacial? 2.2. Quais as principais possibilidades e limitações que visualiza que o Ciberespaço pode colocar à condução das operações militares da NATO?
QD2 - Que possibilidades e vulnerabilidades possui a capacidade de Ciberdefesa da NATO?	3.1. Tendo em consideração os vetores DOTMLPII quais as principais possibilidades/potencialidades (pontos fortes) que identifica na Capacidade da NATO para atuar no Ciberespaço? 3.2. Considerando igualmente os vetores DOTMLPII, na sua perspetiva quais são as principais vulnerabilidades que identifica na capacidade da NATO para atuar no Ciberespaço? 3.3. Em que áreas/vetores visualiza que os aliados possam reforçar a capacidade de atuação no Ciberespaço da NATO?
QD3 - Que possibilidades e vulnerabilidades possui a capacidade de Ciberdefesa das FFAA portuguesas?	4.1. Considerando os vetores de edificação de uma capacidade (DOTMLPII) quais as principais possibilidades/potencialidades (pontos fortes) que identifica na Capacidade nacional em edificação? 4.2. Na sua perspetiva qual o contributo das FFAA portuguesas para a Ciberdefesa da NATO? 4.3. Tendo em consideração a restruturação da capacidade de Ciberdefesa nacional, quais as principais vulnerabilidades que visualiza no seu desenvolvimento e posterior operacionalização?

Apêndice C — Guião de entrevista

ENQUADRAMENTO

O presente TII enquadra-se nas Ciências Militares, na área de técnicas e tecnologias militares, nos termos da alínea c) do n.º 5 do Decreto-Lei n.º 249/2015, de 28 de outubro, mais concretamente no que diz respeito à Evolução da relevância do Ciberespaço para a NATO.

No seguimento do desenvolvimento do tema referido anteriormente, o presente trabalho de investigação terá como principal enfoque a capacidade de Ciberdefesa Nacional, e o seu possível contributo para o reforço da Capacidade Ciber da NATO.

IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	
Posto (se aplicável)**:**	
Cargo/Função:	
Data:	
Local (se aplicável)**:**	
Hora de início (se aplicável)**:**	
Hora do fim (se aplicável)**:**	

QUESTÕES

As questões de seguida apresentadas foram elaboradas tendo por finalidade responder a um conjunto de indicadores, que se entende permitirem atingir o objetivo geral do trabalho. Contudo face á experiência e conhecimentos de Vossa Excelência, as mesmas podem ser alteradas ou sugeridas outras, se entendido por conveniente.

1. O termo ciberespaço, apesar de fazer parte do léxico da vida quotidiana das pessoas e sociedades, potenciado pelos desenvolvimentos tecnológicos, não é consensual, pelo que não há uma definição universal do seu conceito. O termo ocidental ciberespaço é vulgarmente associado à utilização da internet, já em países como a Rússia ou China é denominado como "espaço das informações".
   1.1. Tendo em consideração a sua experiência nesta área, quais as características que destacaria do Ciberespaço?
   1.2. Na sua visão, quais considera serem os desafios e oportunidades mais relevantes que o Ciberespaço apresenta para as pessoas, organizações e sociedades?
   1.3. De acordo com a sua perspetiva quais as principais implicações que o Ciberespaço apresenta às Operações militares?
2. A importância do Ciberespaço para a segurança dos países aliados da NATO, bem como o seu impacto na condução das operações militares, conduziram ao seu reconhecimento, enquanto domínio das operações militares.
   2.1. No seu entender quais as principais razões que levaram a NATO a reconhecer o Ciberespaço enquanto domínio das Operações militares, independente do terrestre, naval, aéreo e espacial?
   2.2. Quais as principais possibilidades e limitações que visualiza que o Ciberespaço pode colocar à condução das operações militares da NATO?
3. De acordo com a doutrina NATO, a edificação de capacidades pressupõe o desenvolvimento dos vetores: Doutrina, Organização, Treino, Materiais, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLPII). A proliferação de equipamentos tecnológicos conectados através da internet, assim como de sistemas baseados em redes, tem moldado de forma decisiva o ciberespaço, o que obriga um constante investimento das organizações para responder às ameaças que dele decorrem, nomeadamente no desenvolvimento de doutrina (normas/regras/procedimentos/tipologia de operações), na obtenção de pessoal qualificado, etc.
   3.1. Tendo em consideração os vetores DOTMLPII quais as principais possibilidades/potencialidades (pontos fortes) que identifica na Capacidade da NATO para atuar no Ciberespaço?
   3.2. Considerando igualmente os vetores DOTMLPII, na sua perspetiva quais são as principais vulnerabilidades que identifica na capacidade da NATO para atuar no Ciberespaço?

3.3. Em que áreas/vetores visualiza que os aliados possam reforçar a capacidade de atuação no Ciberespaço da NATO?

4. A nova LOBOFA, aprovada em 09 de agosto de 2021, conduziu à reformulação da LOEMGFA. Por sua vez a LOEMGFA de 24 de janeiro de 2022 reforça a importância da Ciberdefesa, nomeadamente com a criação de um Comando de Operações de Ciberdefesa, face ao existente Centro de Ciberdefesa (CCD).

4.1. Considerando os vetores de edificação de uma capacidade (DOTMLPII) quais as principais possibilidades/potencialidades (pontos fortes) que identifica na Capacidade nacional em edificação?

4.2. Na sua perspetiva qual o contributo das FFAA portuguesas para a Ciberdefesa da NATO?

4.3. Tendo em consideração a restruturação da capacidade de Ciberdefesa nacional, quais as principais vulnerabilidades que visualiza no seu desenvolvimento e posterior operacionalização?

Apêndice D — Caracterização dos entrevistados

Quadro 3 - Listagem de entidades entrevistadas

Código	Posto /Civil	Nome	Unidade/Entidade	Funções relevantes para a área de investigação	Data	Tipo
E1	BGen	Viegas Nunes	Direção de Comunicações e Sistemas de Informação do Exército.	• Comandante da *NATO Communications and Information Systems School*; • Director da *NATO Communications and Information Academy;* • Coordenador do Grupo de Implementação do *Cyber Academia and Innovation Hub.*	30/03/22	Presencial
E2	Cor	Quaresma Rosa	*NATO Communications and Information Academy.*	Funções atuais.	24/03/22	*Email*
E3	CFR	Vasco Prates	*Cooperative Cyber Defence Centre of Excellence.*	Funções atuais.	01/04/22	*Microsoft Teams*
E4	TCor	Salomão Carvalho	Direção-Geral de Recursos da Defesa Nacional do MDN	• Gestor do projeto *NATO Smart Defence "Multinational Project on Cyber Defence Education and Training (MNCDE&T)";* • Representante nacional no *European Union Military Training Group - Cyber Defence Discipline.*	04/04/22	*Email*
E5	CFR	Câmara de Assunção	Estado-Maior da Armada	• Adj. de Marinha do Chefe do Centro de Ciberdefesa; • chefia da área das tecnologias do CCD; • Divisão de Operações com o núcleo de Ciberdefesa e tecnologias de informação.	07/04/22	*Email*
E6	CMG	Fialho de Jesus	Instituto Universitário Militar do Estado-Maior-General das Forças Armadas	• Chefe do Centro de Ciberdefesa das Forças Armadas; • Representante nacional no *Steering Committee do Cooperative Cyber Defence Centre of Excellence.*	22/03/22	Presencial
E7	CFR	Caldeira Carvalho	Centro de Ciberdefesa do Estado-Maior-General das Forças Armadas	Funções atuais.	29/03/22	Microsoft *Teams*
E8	Maj	Miguel Maria	Estado-Maior da Força Aérea	• Representante da Força Aérea no Comité de Monitorização da Ciberdefesa; • Representante da Força Aérea no Grupo de Trabalho para o Desenvolvimento da Capacidade de Ciberdefesa.	30/03/22	*Email*
E9	Civil	João Farinha	*NATO Communications and Information Academy.*	Funções atuais.	06/04/22	*Email*
E10	S/R	Anónimo	*NATO Cyber Operations Centre*	Funções atuais.	08/04/22	*Email*

Apêndice E — Sinopse das entrevistas

Quadro 4 - Sinopse das entrevistas

	Características do Ciberespaço
E1	*"Tem uma componente física que é a rede que dá acesso"; "tem uma componente virtual, aquilo que é cedido através da componente física"; "é um ambiente eh dual. Portanto tem uma componente física que é o acesso da rede e tem o conteúdo e a e a virtualização que daí decorre"; "O Ciberespaço tem dimensão na sua componente física, que estamos a falar das redes mapeável"; "mas depois tem outra componente não é mapeável que é transversal a todas"; "portanto nós não estamos num espaço tradicional que conseguimos aplicar as mesmas regras"; "Nós estamos num espaço multidimensional"; "mas o possível ciberespaço é verdadeiramente o multiplicador de força, porque nós desenvolvemos capacidades no domínio, e ao mesmo tempo temos a capacidade de atuar e intervir simultaneamente"; "Estou a falar a partir de um domínio atuar simultaneamente sobre todos os outros domínios, o que é absolutamente novo"; "aplicam-se as mesmas regras do comando subordinado é o comando apoiante e apoiado"; "O Ciberespaço pode ser um comando apoiante quando existe uma operação terrestre, pode degradar os sistemas de comando e controlo, acesso às infraestruturas críticas por ataques disruptivos e destrutivos, mas ao mesmo tempo pode ser um comando apoiado"; "O problema da atribuição, ou seja, provar que quem desenvolveu um ciberataque é a pessoa A, B ou C, porque é o princípio para imputar a responsabilidade"; "a resposta dos estados é diferente"; "temos que ir mapear a constituição da república e ver o que é que a constituição da república diz que é a esfera de atuação das Forças Armadas, a soberania do estado, ataque externo, etc., então existe um conjunto de critérios para as Forças Armadas intervirem, portanto nós temos que satisfazer esses critérios".*
E2	*"Para além da componente tecnológica, temos de ter igualmente em consideração as relações sociais e interdependências que são estabelecidas entre indivíduos e entidades através dessas plataformas. Os relacionamentos entre indivíduos e organizações estão cada vez mais dependentes das ligações estabelecidas através do ciberespaço, alargando duma simples interação através de uma conexão primária para ligações secundárias, terciárias, ou mais afastadas ainda... "os amigos dos amigos do amigo". Temos assim um domínio de escala global, sem fronteiras físicas"; "assente numa infraestrutura tecnológica onde reside e circula informação"; "onde se estabelecem relacionamentos entre entidades com distintos ou concorrentes objetivos, mais ou menos alcançados conforme a capacidade de projeção de poder e influências"; "Entidades diferentes, dedicadas a diferentes áreas de atuação, utilizam o ciberespaço com motivações e objetivos distintos e interdependentes, como por exemplo industriais, comerciais e financeiros, políticos e diplomáticos, militares e de segurança, terrorismo, saúde, investigação e desenvolvimento, comunicação social, ou meramente relacionamento interpessoal"; "onde se estabelecem relacionamentos entre entidades com distintos ou concorrentes objetivos, mais ou menos alcançados conforme a capacidade de projeção de poder e influências. Entidades diferentes, dedicadas a diferentes áreas de atuação, utilizam o ciberespaço com motivações e objetivos distintos e interdependentes, como por exemplo industriais, comerciais e financeiros, políticos e diplomáticos, militares e de segurança, terrorismo, saúde, investigação e desenvolvimento, comunicação social, ou meramente relacionamento interpessoal"; "cria uma dependência doentia do ciber. Não sendo um espaço por natureza regulado, é extremamente difícil se não impossível impor normas de conduta na sua utilização"; "pelo que poderá ser utilizado por entidades com fins mais ou menos lícitos"; "Caba a cada utilizador desenvolver os mecanismos de proteção, tecnológicos ou processuais, que lhes permita uma "navegação" segura neste espaço e aos estados desenvolver normativos legais e estruturas para garantir o cumprimento das aceitáveis normas de conduta".*
E3	*"o que conseguimos observar num determinado momento e num determinado espaço altera-se muito rapidamente"; "Deveremos ter em consideração a sua acessibilidade, se tendencialmente temos a ideia que as armas só estão acessíveis a determinados grupos de pessoas, ou grupos restritos de entidades, no ciberespaço já não é assim"; "Uma outra característica que lençaria prende-se com a sua transversalidade, pois ele atravessa todos os outros domínios tradicionais"; "é uma construção humana"; "é complexo, pelo que não se consegue antever qual o resultado quando se provoca um efeito, quer dizer nem sempre o output é o mesmo, e por vezes é mesmo inesperado".*
E4	*"o ambiente de valores e interesses complexo"; "área de responsabilidade coletiva"; "que resulta da interação entre pessoas, redes e sistemas de informação"; "marcado por um ritmo acelerado da transformação digital"; "interdependência"; "a capacidade de usufruir do ciberespaço em segurança e em liberdade está a tornar-se cada vez mais relevante e central para o desenvolvimento das sociedades modernas. Através do ciberespaço existem organizações que já foram atacadas, as que estão sob ataque e que o desconhecem, e as que sabem que sertão atacadas desconhecendo quando acontecerá. A desigualdade digital continua a ser muito relevante em termos de risco global"; "utilização de instrumentos não militares"; "ameaças cyber e hibridas, em diferentes situações de conflito"; "Num ambiente de Guerra Hibrida os Estados*

	passaram a moldar o ambiente de informação, com a condução da guerra no ambiente de informação"; "tirando o partido de um aparente anonimato, e sem violar as leis internacionais sobre a soberania de outros Estados"; "deve ser abordada de forma inclusiva, alargada e integradora, promovendo a indispensável cooperação entre instituições civis e militares"; "elemento integrante do processo de planeamento estratégico e operacional": "deverá ser dada especial atenção à sua potencial influência nas missões e nos outros domínios de operações"; "A Ciberdefesa participará no conjunto das operações de defesa numa perspetiva multi-dominio (terra, mar, ar, espaço e ciberespaço)"; "constituindo-se igualmente como um elemento de dissuasão"; "obedecendo à mesma lógica e fundamentos que caracterizam a atuação em operações cinéticas"; "processo credível de imputação da entidade responsável pelo ataque"; "legitimidade e credibilidade".
E5	*"um domínio virtual global"; "constituído por computadores"; "sistemas de informação e redes de comunicações interligadas e inter-relacionadas, no qual o elemento mais valorizado é a informação que nele é armazenada, transmitida e processada"; "dimensão e complexidade do que é realmente o ciberespaço"; "componente ciber em conjunto com a componente da guerra da informação, interligando claramente estas duas componentes"; "facto de ser um espaço sem limites físicos de fronteiras"; "ser passível de ser percorrido entre dois pontos fisicamente distantes em milésimos de segundo"; "ter sido pensado e edificado pelo Homem"; "ausência do que possam ser consideradas fronteiras físicas"; "permitindo que o adversário possa estar permanentemente "próximo" do que possa ser considerado ciberespaço "amigo".*
E6	*"uma camada física constituída pelo hardware, pelos computadores e outros equipamentos; uma camada lógica que corresponde à informação armazenada no ciberespaço"; "e uma camada denominada de pessoal, que corresponde às interações entre as pessoas através do ciberespaço"; "ausência de fronteiras, onde uma ação provocada num ponto do mundo pode ter consequências quase instantâneas noutro ponto do planeta. Uma outra característica prende-se com a grande dependência das pessoas deste domínio, desde os pequenos aparelhos de utilização diária, até aos serviços providenciados por diversas organizações (bancos, serviços públicos, et). A possibilidade de anonimato dos atores que atuam no ciberespaço é também uma característica única deste domínio, o que na maioria das vezes dificulta a imputação das responsabilidades"; "Verifica-se igualmente uma profusão de novos atores neste domínio, nomeadamente atores estatais, não-estatais, hakers, etc"; "Parece-me importante referir que uma característica fundamental do ciberespaço é o sentimento de impunidade, provocado pela possibilidade de anonimato"; "dificuldade de imputação de responsabilidade. A assimetria marca também o ciberespaço, uma vez que o recurso a um computador ligado à internet tem a capacidade de provocar danos em estruturas críticas de um país, em todo o mundo"; "o triângulo Velocidade – Tempo – Alcance, que faz aumentar a surpresa de um ataque, reduzindo o intervalo de tempo que as organizações possuem para responder de forma adequada".*
E7	*"é um global comum que afeta toda a sociedade, todo o mundo direta e indiretamente"; "Mesmo em lugares remotos há uma total dependência do ciberespaço"; "As características que mais se releva do ciberespaço são o facto de se considerar que não possui fronteiras"; "que não existe jurisdição"; "O ciberespaço não tem espaço físico"; "fazem parte do computador de alguém, que se encontra num espaço físico"; "a nuvem está dividida por vários países"; "faz com que se apliquem diferentes leis em vigor nesses locais"; "No ciberespaço é difícil impor consequências a quem infringe as leis"; "embora se tenha evoluído muito, mas mais dedicado a crimes graves"; "O ciberespaço não tem fronteiras porque é difícil delimitar os utilizadores individualmente, sem restringir as liberdades e os direitos das pessoas"; "Destacaria igualmente o anonimato do utilizador, ou seja, a capacidade para esconder a pegada digital de tudo lá é efetuado, para o bem e para o mal.*
E8	*"a camada física"; "camada lógica"; "camada ciberpersona"; "A camada física é constituída essencialmente por toda a infraestrutura de comunicações e os dispositivos das Tecnologias de Informação e Comunicação"; "que permitem aceder à informação por intermédio da camada lógica do ciberespaço"; "camada lógica, esta é constituída por um conjunto de regras (endereçamento, protocolos, etc.) que permitem interligar os diversos elementos da camada física entre si de forma abstrata"; "a camada ciberpersona representa a identidade digital que os diversos atores (humanos ou não humanos) assumem no ciberespaço"; "um mesmo ator poderá assumir diferentes personalidades no ciberespaço (ex. perfil nas redes sociais, conta de e-mail, conta de acesso a uma determinada página web, etc.) "; "Na maioria das vezes as ações e os danos provocados por um ataque não são visíveis"; "Não está condicionado por limites fronteiriços, pois é agnóstico à distância em virtude de uma determinada ação poder estar à distância do pressionar de um botão"; "Permite que os diversos atores se relacionem entre si independentemente da camada física"; "No ciberespaço não tem de haver superioridade em relação ao adversário, basta apenas o conhecimento necessário para se poder explorar uma determinada vulnerabilidade existente"; "No ciberespaço os tempos de aviso e reação são muito mais rápidos comparativamente com os restantes domínios clássicos"; "exige uma tomada de decisão mais célere"; "é possível aceder a grandes quantidades de informação de forma quase imediata"; "A maioria das regras aplicáveis aos conflitos que decorrem nos domínios clássicos não têm aplicabilidade no ciberespaço"; "existem diferentes interpretações sobre a legitimidade dos atos praticados, bem como uma multiplicidade de atores"; "tem de se lidar com a problemática da atribuição das ações"; "torna mais critico atendendo ao fator tempo.*

E9	*"que se expande para além daquilo que é conhecido como a Internet"; "todos os sistemas de comunicações e tecnologias de informação"; "sistemas eletrónicos, as redes"; "sistemas eletrónicos, as redes".*
Desafios e oportunidades do Ciberespaço	
E1	***Desafios:*** *"sob o ponto de vista da doutrina militar é o maior desafio que nós temos pela frente"; "é por isso que o Ciberespaço tem progredido tão devagar em termos doutrinários, em termos de emprego operativo e operacional tem levado mais tempo do que seria desejável o seu caminho".*
E2	***Desafios:*** *"o grau de confiança e verossimilhança da informação e das fontes"; "a seleção da informação relevante e oportuna para apoio à decisão"; "a capacidade tecnológica para processar grandes volumes de informação e torná-la utilizável"; "a capacidade de atualização tecnológica à velocidade da relevância"; "garantir a segurança da informação e resiliência"; "promover o conhecimento"; "consciência dos riscos associados à dependência do ciberespaço e como mitigá-los".* ***Oportunidades:*** *"encurtar distâncias físicas e temporais, estabelecer relacionamentos interculturais e aproximar sociedades, acesso ilimitado e partilha de informação"; "a um ritmo acelerado e num domínio ativo 24 horas por dia onde de qualquer lugar se pode aceder e estabelecer interações com outro ser digital. Um dos grandes desafios para as entidades é a obtenção no momento oportuno da superioridade de informação que lhes permitirá ganhar vantagem sobre um competidor e gerar valor"; "acesso oportuno à informação, avaliar a que é relevante ou acessória, processa-la, dissemina-la, negar o acesso ou manipular a informação disponível às restantes entidades que competem pelo mesmo espaço"; "apresenta como oportunidades o acesso a grandes volumes de informação"; "a possibilidade de estabelecer ligações intrincadas com uma imensidão de atores".*
E3	***Desafios:*** *"dificuldade que é gerir os dados, a informação e conhecimento gerados no ciberespaço"; "a legislação, não procurando justificar a sua necessidade ou não, a verdade é que a sua necessidade é reconhecida, contudo existe uma enorme dificuldade em legislar o Ciberespaço.* ***Oportunidades:*** *"acessibilidade aos dados, à informação e ao conhecimento"; "É um meio que permite recolher dados e assim construir informação e conhecimento"; "também o ciberespaço possui já bases de conhecimento que podem ser exploradas"; "referiria a velocidade como se pode obter conhecimento como uma oportunidade para as pessoas e sociedades. A ausência de limites geográficos permite também expandir o conhecimento por extensos espaços geográficos, o que contribui para o aumento da globalização".*
E4	***Desafios:*** *"domínio central ao desenvolvimento humano, social, cultural e económico, entre outros"; "um espaço onde operam indivíduos, entidades e Estados com agendas desestabilizadoras, realizando ações de natureza encoberta, assimétrica e híbrida"; "comprometem a segurança, a confiança e a liberdade do uso – justo, equilibrado, partilhado e global – desse espaço coletivo da humanidade"; "devem ser asseguradas a partilha de informação, por todas as entidades técnicas com responsabilidades na segurança do ciberespaço"; "avaliação conjunta da natureza e extensão das ameaças"; "garantindo uma identificação precisa de todos os incidentes e ataques de natureza estatal ou não estatal no ciberespaço ou através dele, ou com impacto na soberania e/ou na resiliência estrutural do Estado"; "Deve ser reforçada a importância que a segurança do ciberespaço tem na vida das pessoas e das organizações"; "O emergir de novas e velhas ameaças, fruto de uma maior necessidade de utilização do digital e da crescente exposição às suas vulnerabilidades"; "uma maior segurança no ciberespaço"; "autonomia tecnológica"; "formulação de doutrina, políticas, normas e procedimentos indispensáveis a este novo domínio de operações"; "Os agentes de ameaça no domínio do ciberespaço podem ter como veículo as tecnologias emergentes e disruptivas, da supercomputação, da robótica e da inteligência artificial".* ***Oportunidades:*** *"linha com o princípio de cooperação"; "utilização do ciberespaço é uma condição essencial para o processo das informações, para o processo cooperativo e para uma transição digital bem-sucedida. A sensibilização e a capitalização do conhecimento nacional e dos cidadãos nesta área assumem especial importância"; "fundamental o desenvolvimento das melhores ferramentas e capacidades para as contrariar, nomeadamente através de parcerias com centros de investigação e desenvolvimento, universidades e empresas".*
E5	***Desafios:*** *"Como em qualquer "oásis", tal como pode ser descrito o ciberespaço, encontram-se sempre desafios ocultos e perigos que decorrem exatamente desta liberdade que o ciberespaço proporciona"; "A possibilidade de atores maliciosos facilmente mistificarem a sua presença no ciberespaço constitui um dos maiores desafios à segurança, principalmente no que diz respeito à capacidade de as autoridades poderem efetuar a identificação e atribuição dos ataques no ciberespaço"; "A ausência de um entendimento à escala global sobre a governação e regulação da internet caracteriza este espaço virtual como o "digital far west" "; "A facilidade com que os eventos acontecem no ciberespaço pode ser catalisado pelos atores em proveito próprio, trazendo para a esfera da segurança uma necessidade de monitorização constante dos sistemas para uma resposta eficaz".*

	Oportunidades: *"é a perspetiva de uma sociedade mais globalizada onde é possível a troca de informação e partilha de experiências de uma forma muito simples"; "recorrendo a dispositivos que podem andar no bolso de cada indivíduo e contribuindo para que as pessoas possam trabalhar em locais fisicamente remotos das suas equipas".*
E6	***Desafios:*** *"crescente aumento da dependência da sociedade pela componente tecnológica, a dificuldade na sua regulação"; "inovação tecnológica atual está superando a capacidade dos Estados em acompanhar os desenvolvimentos e os seus potenciais impactos sociais"; "caso um governo estabeleça regras tendo em vista gerir esses efeitos, o alcance global de muitas tecnologias emergentes e seus impactos exigem novas abordagens de governança multilateral, o que torna mais complicada a resposta dos Estados. E convém não esquecer as diferenças culturais (Ocidente vs China e Rússia), que poderão ser fatores de atrito nesta dimensão".* ***Oportunidades:*** *"às oportunidades se evidenciam as possibilidades de desenvolvimento social e económico"; "da melhoria dos processos organizacionais e do acesso e disseminação do conhecimento".*
E7	***Desafios:*** *"como também para o crime"; "passamos de hakers curiosos para descobrir até conseguiam ir, para grupos criminosos organizados".* ***Oportunidades:*** *"Permite ter uma loja virtual numa garagem, onde se produzem artigos artesanais, e depois são vendidos a nível mundial"; "Potencia negócios que dificilmente seriam desenvolvidos"; "onde a simples partilha de um vídeo no Youtube potencia a criação de uma empresa, ou de uma marca"; "na prática potencia a globalização"; "estando tudo à distância de um click"; "O ciberespaço é um mundo de oportunidades para os negócios".*
E8	***Desafios:*** *"as pessoas, organizações e sociedades tornaram-se de forma progressiva extremamente dependentes do ciberespaço. O nosso atual modelo de sociedade conduziu-nos a uma total dependência do ciberespaço, pois a internet está presente na maioria das nossas tarefas do dia a dia"; "Dado o elevado grau de dependência da internet e de outros segmentos de rede"; "utilização segura e livre do ciberespaço. Considerando as ameaças existentes no ciberespaço, perpetradas pelos mais diversos atores, designadamente Cibercriminosos, Hackers, Ciberativistas, Crimeorganizado"; "torna-se necessário garantir a segurança dos recursos utilizados para acesso ao ciberespaço, através de uma evolução permanente dos sistemas"; "garantir uma cultura de segurança dos próprios utilizadores"; "evitar as ameaças presentes no ciberespaço"; "acautelar a própria ameaça interna de ações praticadas deliberadamente ou inadvertidamente pelos próprios colaboradores de uma determinada organização"; "ações desencadeadas no ciberespaço por atores estatais ou não estatais"; "destinadas a degradar de forma deliberada a capacidade de utilização do ciberespaço parte de organizações e ou países terceiros, seja por motivos políticos, económicos ou outros"; "a segurança constitui um dos principais desafios"; "educação e sensibilização dos utilizadores"; "combate ao cibercrime"; "dependência do ciberespaço".*
E9	***Desafios:*** *"Os reguladores, por seu lado, não conseguem acompanhar essa evolução, e chegam na maioria dos casos "atrasados" aos processos"; "Tudo isto cria uma dependência extrema no ciberespaço"; "faz com que algumas organizações tenham reunido capacidades globais que ultrapassam a que a maioria das Nações possuem".* ***Oportunidades:*** *"Se até ao desenvolvimento do ciberespaço as inovações ocorriam ao longo de gerações (e mesmo uma inovação recente como a aviação ocorreu ao longo de 3 ou 4 gerações, o que a uma escala da humanidade é um período extremamente curto), observamos agora transformações que ocorrem em menos de 10 anos"; "potenciador de lucro e de desenvolvimento".*
E10	***Desafios:*** *"Por outro lado, a defesa contra ataques cibernéticos requer cooperação entre organizações internacionais, governos e indústria"; "acredito que é realmente um desafio "orquestrar" atividades cibernéticas entre pessoas, organizações e sociedades".*
Implicações do Ciberespaço nas Operações militares	
E1	*"Hoje a liderança é eminentemente digital, é à distância, passámos o tempo em que o comando era à voz, era o general no meio do campo de batalha"; "O General manifesta-se por contacto remoto, pode ter um elã enorme, mas é contacto remoto está lá a vertente do ser humano nisto".*
E2	*"Sendo um domínio individualizado, onde é possível planear a produção de efeitos, é também um domínio transversal uma vez que todos os outros assentam no ciberespaço para recolha de dados, produção de informações, tomada de decisão, planeamento, emprego de meios, coordenação, comunicações e comando e controlo"; "quem detiver superioridade neste domínio, quer para defesa e proteção ou para produção de efeitos, terá logo à partida vantagem operacional. Cada vez mais o ciber terá que ser contemplado no desenvolvimento das capacidades militares"; "devem ser consideradas implicações de natureza ciber que permitam potenciar vantagem e reduzir riscos"; "o conhecimento do ambiente informacional e ameaça ciber nos processos de planeamento é essencial para avaliar o nível de risco e decidir a forma de emprego de qualquer meio que é "IP enabled" "; "tem de estar consciente dos riscos e ameaças e treinado nos mecanismos/procedimentos de mitigação e reforço de segurança da informação"; "o material e soluções tecnológicas devem comtemplara mecanismos de proteção e garantia da segurança da informação e resiliência"; "o material e*

	soluções tecnológicas devem comtemplara mecanismos de proteção e garantia da segurança da informação e resiliência"; "A negação de acesso á informação pode influenciar o desenvolvimento de capacidades assim como reduzir o conhecimento situacional e impactar a oportunidade de emprego. A capacidade de moldar o ambiente informacional com campanhas de desinformação, pode certamente impactar a vontade (aceitação) de aplicação dos meios. O ciberespaço é assim o domínio operacional que nos permite influenciar o ambiente informacional"; "Cada vez se torna mais comum que os "fogos de preparação" e as operações de moldagem sejam conduzidas através do ciberespaço"; "Conflitos recentes mostram o volume de ações no ciberespaço de negação de disponibilidade de serviços, de controlo de plataformas de controlo de fogos de artilharia, de ações de engenharia social e campanhas de desinformação, a acontecerem muito antes das ações mais cinéticas do conflito".
E3	*"mobilidade dos meios ou dos alvos. Os meios que pensamos ter disponíveis para uma determinada operação deixam de estar disponíveis, e há uma elevada mobilidade na sua utilização como na aquisição dos alvos. A sincronização das ações, é muito importante sincronizar as ações no ciberespaço com as ações nos outros domínios"; "A relação de eficiência Vs segurança, podemos pensar que temos um sistema muito seguro, mas que pode limitar a eficiência das ações"; "os alvos das ações no ciberespaço não são dedicados especificamente aos meios militares, mas sim aquilo que classificamos como mission enablers, "; "se for o caso a NATO, ao serem planeadas e conduzidas as operações militares, onde o ciberespaço seja considerado, todos os efeitos criados nesta dimensão são da responsabilidade das nações em apoio ao comandante operacional".*
E4	*"As Forças Armadas dependem cada vez mais da utilização do ambiente de informação e do próprio ciberespaço para conduzir todo o espetro de operações"; "condução de operações de e através do ciberespaço procurando tirar com eficácia a superioridade de informação"; "devem ser executadas no respeito do quadro legal em vigor"; "sempre em linha com o Direito nacional e internacional aplicável"; "deverá reger-se sobretudo pelos princípios da proporcionalidade e da necessidade"; "princípios regentes do Direito internacional humanitário".*
E5	*"o maior facilitador da capacidade de comando e controlo (C2) numa operação militar"; "sem uma capacidade de C2 efetiva não é possível a condução de operações de uma forma eficaz, pelo que este domínio é essencial no âmbito militar para a condução de operações"; "O garante da segurança de toda a informação que é transmitida, armazenada e processada no ciberespaço, assegura em grande parte o cumprimento da missão de uma força militar, garantindo a todo o momento a confidencialidade, integridade e disponibilidade da informação que irá contribuir para a tomada de decisão das chefias militares".*
E7	*"nunca foi tão eficaz o nevoeiro da guerra"; "nunca foi tão eficaz o nevoeiro da guerra"; "Acima de tudo porque o ciberespaço pode afetar todas as infraestruturas críticas de um país"; "Veja-se o caso da Ucrânia, onde afetou a luz, na Estónia desligaram os serviços públicos"; "A exploração de uma simples vulnerabilidade nos sistemas pode provocar impactos cinéticos gigantescos".*
E8	*"todos os domínios clássicos recorrem a este domínio para a condução das suas operações"; "um Comandante deverá ter capacidade para negar a utilização do ciberespaço por parte do adversário a fim de garantir o sucesso das suas operações"; "o Comandante Militar deverá considerar seriamente esta capacidade no âmbito de uma operação"; "o Comandante Militar deverá considerar seriamente esta capacidade no âmbito de uma operação"; "devem ser adotadas Regras de Empenhamento específicas para este domínio".*
E9	*"Qualquer sistema de comunicações ou de comando e controlo depende do ciberespaço"; "existe o efeito indireto que a exploração do ciberespaço enquanto meio de comunicação de massas pode surtir na moral dos militares e da sociedade em geral (onde entram as campanhas de desinformação que são claramente observáveis nos conflitos recentes)"; "ataques às funções elementares da sociedade (como a banca, os serviços públicos, o retalho, o abastecimento de energia ou de água, entre outros)".*
E10	*"O ciberespaço tem o potencial de prejudicar as nossas economias"; "O ciberespaço tem o potencial de prejudicar as nossas economias"; "informações significativas para apoiar nossos líderes/comandantes na tomada de decisões"; "Do ponto de vista da defesa, no passado, uma mentalidade militar de operações conjuntas era suficiente, mas agora uma abordagem multi-domínio é absolutamente necessária"; "O ciberespaço precisa ser integrado, mas também sincronizado com os outros domínios para obter efeitos operacionais".*
Razões que levaram a NATO a reconhecer o Ciberespaço como um domínio das Operações	
E1	*"um ataque no ciberespaço também poderá, no limite, iniciar uma resposta ao abrigo do Artigo 5. da Aliança"; "nós podemos falar em apoio de fogos no Ciberespaço, podemos falar em economia de forças podemos falar em liberdade de ação, podemos falar em unidade de comando, unidade de esforço tudo isto se aplica no Ciberespaço";*

	"é um domínio diferente dos outros"; "Portanto, se eu os tenho um Quartel-General para as forças terrestres, para as forças aéreas e navais, tenho que ter um Quartel-General para o Ciberespaço, portanto tem que ter um Comando"; "é porque é um vetor de exercício de poder, como os outros".
E2	*"domínio transversal"; "todos os restantes dependem para o planeamento, consecução e execução do comando e controlo"; "ele próprio um domínio onde podem ser conduzidas ações para a produção de efeitos tão ou mais devastadores que ações cinéticas dos outros domínios"; "Todos os conceitos de emprego do poder militar nos restantes domínios podem ser aplicados ao ciberespaço.*
E3	*"a condução das operações no ciberespaço pode ser efetuada de forma independente dos restantes domínios, ou seja, para efetuar uma operação no ciberespaço não é necessário conduzir operações aéreas ou terrestres"; "Um outro fator prende-se com o facto deste domínio estar sempre a ser contestado, havendo sempre atores a desenvolver ações coercivas ou destrutivas, independentemente dos outros domínios"; "Se pensarmos as tarefas que a NATO desenvolve, estas ações podem afetar todas as tarefas e missões da NATO, e por tanto a NATO teria que fazer alguma coisa*
E4	*"transversal a qualquer um dos outros domínios operacionais"; "qualquer equipamento ou tecnologia utilizada nos diferentes domínios está, de certa forma, ligada à utilização do ciberespaço"; "evolução em complexidade e nível de sofisticação dos ataques que têm vindo a ser desenvolvidos no âmbito do ciberespaço"; "sendo a NATO um alvo atrativo para os seus adversários"; "os aliados devem defender-se de uma forma eficaz como o fazem nos restantes domínios".*
E5	*"alterações e transformações muito rápidas"; "ser relativamente fácil recorrer à mistificação dos atores"; "um espaço de utilização livre, sem qualquer tipo de regulação"; "os potenciais adversários da Aliança já o incorporavam nas suas doutrinas militares como tal, podendo ficar para trás caso não se preparasse para realizar operações militares neste domínio".*
E6	*"O principal motivo prende-se com a dependência das sociedades do ciberespaço"; "do impacto que os ciberataques podem ter nos países aliados"; "São vários os exemplos internacionais onde o ciberespaço foi utilizado para fins de afirmação política ou no contexto da geoestratégia".*
E8	*"as capacidades do domínio do ciberespaço podem produzir efeitos, de forma independente dos outros domínios. O que esteve na base do reconhecimento do ciberespaço, enquanto domínio das operações militares foram os ciberataques"; "Ficou provado que através de operações no ciberespaço é possível produzir efeitos e inclusive alcançar objetivos militares"; "a NATO continuou a acompanhar evolução das ameaças provenientes do ciberespaço que foram se tornando cada vez mais frequentes, complexas e impactantes"; "os diversos Chefes de Estado e de Governo dos estados membros da Aliança Atlântica reconheceram que o Direito Internacional é aplicável ao ciberespaço, pelo que a Ciberdefesa constitui um dos objetivos de defesa coletiva da Aliança".*
E9	*"reconhecimento da importância de garantir a segurança do ciberespaço, enquanto parte indissociável das operações militares atuais e futuras"; "oportunidade de desenvolver novas capacidades para operar no ciberespaço"; "um ataque no ciberespaço também poderá, no limite, iniciar uma resposta ao abrigo do Artigo 5. da Aliança".*
Possibilidades e limitações às Operações da NATO	
E1	***Limitações:*** *"Não é um problema de ferramentas não é um problema de ligações é um problema conhecimento".*
E2	***Possibilidades:*** *"O sucesso operacional da NATO, como de qualquer outro ator, encontra-se diretamente dependente da capacidade de estabelecer superioridade neste domínio operacional"*
E3	***Limitações:*** *"resulta de um domínio altamente competitivo no qual a Aliança terá que encontrar soluções para a sua exploração em confronto com os seus adversários"; "A NATO nunca consegue ter o terreno preparado para desempenhar uma ação."; "como sabemos noutras zonas do globo não existem tantas restrições de atuação no ciberespaço, e isto poderá ser uma limitação à condução das operações pela NATO".*
E4	***Possibilidades:*** *"a ciberdefesa participa no conjunto das operações da defesa numa perspetiva multi-domínio (terra, mar, ar, espaço e ciberespaço)"; "constituindo-se igualmente como um elemento de dissuasão"; "Um grande passo está a ser dado pela NATO, através da iniciativa DIANA"; "domínio de capital intelectual intensivo e que vive muito da inovação tecnológica e da utilização massiva e continua das Tecnologias Emergentes e Disruptivas (EDT)".*
E5	***Limitações:*** *"resulta de um domínio altamente competitivo no qual a Aliança terá que encontrar soluções para a sua exploração em confronto com os seus adversários".*
E6	***Possibilidades:*** *"os ciberataques estão associados a efeitos menos destrutivos".*

	Limitações: *"Sendo o ciberespaço um "enabler", isto tem aplicabilidade nas outras dimensões, na medida em que os sistemas são cada vez mais tecnológicos, assim como toda a componente de planeamento e execução logística. E quando falamos de comando e controlo, nos dias de hoje, com o crescente tecnológico na sua conceção, naturalmente que a dependência do ciberespaço é maior".*
E8	***Possibilidades:*** *"as operações no ciberespaço podem permitir aumentar o conhecimento situacional sobre forças opositoras da Aliança Atlântica"; "permitem alcançar determinados efeitos sem necessidade de colocar tropas no terreno, dai a necessidade de integrar o ciberespaço no processo de planeamento operacional"; "a NATO criou o Cyber Operations Centre (CyOC) em 2018, com o objetivo de integrar os efeitos no ciberespaço no processo de planeamento estratégico e operacional".* ***Limitações:*** *"qualquer ação destinada a produzir efeitos fora do seu ciberespaço, terá de ser solicitada a um estado-membro da Aliança através do mecanismo Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)"; "é possível identificar com clareza as forças opositoras, pois existem muitos atores não estatais, alguns deles patrocinados por estados que visam interferir com os objetivos da Aliança Atlântica"; "em futuros conflitos importa garantir a superioridade no ciberespaço".*
E9	***Possibilidades:*** *"possibilidade de causar efeitos com um impacto moderado"; "os ciberataques estão associados a efeitos menos destrutivos".*
E10	***Possibilidades:*** *"A consciência situacional abrangente do ciberespaço informa os objetivos das missões e as operações defensivas do ciberespaço tornam nossas missões mais resilientes"; "Além disso, integração dos efeitos cibernéticos com todos os efeitos operacionais".* ***Limitações:*** *"Áreas cinzentas em funções, responsabilidades e autoridades".*
Pontos Fortes da Capacidade de Ciberdefesa da NATO	
E1	*"O ponto forte da capacidade Ciber é educação"; "e treino"; "E o material"; "Organização"; "doutrina"; "treino"; "liderança"; "Tu precisas de pessoal porque o pessoal tem o conhecimento, não é soldados de infantaria na frente, bota no terreno, é mais do que isso, são pessoas qualificadas, e qual é o fator diferenciador"; "A doutrina que sai aprovada pela NATO é uma doutrina consensualizada entre os vários estados, entre os vários países"*
E2	*"O pessoal encontra-se treinado e extremamente motivado para o desempenho das suas funções"; "a existência de uma plataforma de partilha permanente de informação que possibilita ter um alerta antecipado e permanente sobre ameaças e vulnerabilidades dos sistemas"; "uma estrutura capaz de coordenar a intervenção de apoios entre nações"; "condução quer de exercícios conjuntos onde o ciberespaço é o principal domínio operacional, testando interoperabilidade técnica e processual, mas também exercícios conjuntos e combinados onde as considerações ciber se encontram presentes na construção dos cenários e nos processos de planeamento das operações"; "disponibilização de maios humanos para as estruturas existentes cna NATO"; "Ganha a NATO pois consegue ter os recursos humanos necessários"; "a rede de contactos e relacionamentos interpessoais que daí podem advir traduzem uma mais valia para a solução e mutuo apoio internacional quando uma situação de crise surgir"; "A rede de conhecimentos pessoais e organizacionais que se estabelece pode fazer a diferença no tempo de resposta e limitação de danos"*
E3	*"O treino"; "o Material e o pessoal"; "Muitas nações possuem pessoal muito bem treinado e preparado, com muito conhecimento"; "Existe igualmente muitas infraestruturas que possibilitam esta linha de treino"; "A interoperabilidade tem sido também uma grande aposta da NATO".*
E4	*"impulsionado pela capacidade de utilização de soluções inovadoras de duplo-uso e das EDTs"; "uma resposta all-of-state na arena civil e militar, exigindo uma workforce altamente qualificada"; "capacidade de partilha de informação entre os seus Aliados"; "eliminação das eventuais lacunas existentes nos estados com menor capacidade, pelas verdadeiras potências neste domínio"; "a utilização da capacidade ofensiva, como um elemento de dissuasão".*
E5	*"Doutrina"; "Organização"; "A Doutrina como base para todas as fases das operações militares é fundamental e nos últimos anos a Aliança tem levado a cabo um esforço no sentido de edificar este vetor"; "produção de ciber-efeitos tendo para tal sido desenvolvida a framework de contribuição voluntária das nações para a produção de efeitos no, e através do, ciberespaço, SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies) "; "saliento a edificação do Cyberspace Operations Centre (CyOC) no SHAPE com vista à condução das operações militares no ciberespaço, bem como a integração da componente do ciberespaço nas multi-domain operations".*
E7	*"eu diria que o as tem infraestruturas"; "organização"; "doutrina".*
E8	*"Allied Joint Doctrine for Cyberspace Operations – AJP-3.20, Standing Operating Procedures do CyOC entre outros documentos aprovados pelo NATO Atlantic Council"; "Implementação do CyOC para com o objetivo de integrar os efeitos no ciberespaço no processo de planeamento estratégico e operacional"; "apoiar o SACEUR nas questões relativas a este novo domínio de operações"; "a NATO proporciona treino através da participação de cursos de formação realizados na NATO School e na NCI Academy, ou em parceria com o CCDCOE Tallinn"; "a NATO promove a realização periódica exercícios, designadamente o Cyber Coalition, bem como outros em parceria com o CCDCOE Tallinn, nomeadamente o Locked Shields e o Crossed Swords, que contam a participação de países da Aliança Atlântica e alguns países parceiros*

	da NATO"; "a NATO possui os recursos materiais necessários para conduzir operações no ciberespaço"; "O CyOC foi constituído na dependência do Cyberspace Directorate, que por sua vez está na dependência do SACEUR, pelo que em termos de liderança está perfeitamente estabelecida a linha de Comando"; "a NATO possui os recursos humanos qualificados necessários para conduzir operações no ciberespaço"; "a NATO possui os recursos humanos qualificados necessários para conduzir operações no ciberespaço"; "julgo que a NATO possui as condições necessárias"; "Existem algumas iniciativas para garantir interoperabilidade entre a NATO e os Estados membros da Aliança".
E9	*"Doutrina"; "Organização"; "Treino"; "Esta forte componente doutrinária faz com que, por exemplo, apesar da pressão em ligar cada vez mais dispositivos à Internet (inclusivamente por parte dos respetivos fabricantes), a NATO tenha conseguido manter a segregação física da sua informação mais sensível, mantendo-a isolada da Internet"; "leva a que tenha sido desenvolvido o mecanismo "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)", em que a NATO poderá procurar nações que voluntariamente produzam efeitos no ciberespaço, em coordenação com o comandante operacional de uma força"*
E10	*"A infraestrutura de TI da OTAN cobre mais de 60 locais diferentes, desde a sede política em Bruxelas até os comandos militares e locais de nossas operações"A NATO realiza exercícios de interoperabilidade e operações cibernéticas, incluindo os oficiais de bandeira, bem como a camada política e compartilhando as melhores práticas com os Parceiros".*
Vulnerabilidades da Capacidade de Ciberdefesa da NATO	
E1	*"São pessoas com competências, a maior a maior dificuldade"; "A NATO tem um problema, a NATO não é um país são vários países"; "Portanto as doutrinas nacionais existem, algumas mais dominantes do que outras, a doutrina dos Estados Unidos que tem um peso, vamos assim chamar superior à dos outros países, há o Reino Unido que também tem uma doutrina normalmente alinhada ou mais madura ainda do que do dos Estados Unidos, e depois tudo isto tem que jogar junto não é? "; "quem influencia a doutrina é quem tem mais força"; "Os Estados Unidos têm um peso superior aos demais países porque é quem dá um maior contributo para a NATO, e a partir daí aquilo que são os seus drivers, conceitos e doutrina são seguidos"; "tudo isto, em termos de ajustamento, deriva da capacidade que nós tivemos de integrar a velocidade e a agilidade dos países dentro daquilo que é o coletivo da NATO porque a velocidade Ciber é estonteante"; "os efeitos ofensivos da NATO neste domínio não são produzidos pela NATO"; "isto pressupõe haja um alinhamento doutrinário, senão não vai funcionar".*
E2	*"tem presente que não consegue proteger as redes da NATO sozinha"; "é necessário o estabelecimento de colaboração e cooperação entre entidades similares de nações aliadas"; "existe a necessidade de partilha permanente de informação sobre ameaças, riscos e sobre formas de mitigação e recuperação"; "Não existindo forças da NATO, mas sim contribuições nacionais para operações no âmbito NATO, também a produção de efeitos no ciberespaço por parte da NATO está limitado à contribuição dos paises aliados"; "a NATO depende das capacidades desenvolvidas"; "do pessoal treinado por esses países"; "qualquer decisão ao nivel NATO, é o facto da decisão ser por consenso a 30 nações"; "É impensável em incidentes de larga escala, uma entidade, ou nação, que consiga responder a um incidente no ciberespaço sem que tenha de procurar apoio em outros estados ou organizações"; "É impensável em incidentes de larga escala, uma entidade, ou nação, que consiga responder a um incidente no ciberespaço sem que tenha de procurar apoio em outros estados ou organizações"; "Para a produção de efeitos no ciberespaço (ciber operações) a NATO pode utilizar os meios oferecidos por 7 nações que declararam a sua disponibilidade para a condução deste tipo de operações em nome da NATO".*
E3	*"A dificuldade em obter recursos qualificados é uma dificuldade transversal a todos os países aliados da NATO"; "prende-se com o vetor doutrina"; "o vetor organização"; "e o vetor Liderança. Enquanto a liderança está mais ou menos colmatada"; "de doutrina"; "organização não"; "dificulta a obtenção de uma harmonização da organização e da doutrina é bastante complexo. Incluo também nestas limitações a realização das operações ofensivas, nomeadamente a dependência da oferta por parte dos aliados".*
E4	*"As vulnerabilidades estarão sempre ligadas à existência de recursos humanos suficientes, e com as competências adequadas"; "domínio de capital intelectual intensivo"; "partilha de informação entre os seus Aliados"; "associada ao facto de ser uma aliança defensiva e quando a capacidade ofensiva terá que ser disponibilizada pelos seus aliados".*
E5	*"por força da necessária interoperabilidade entre Aliados e a Aliança para a prossecução de operações militares conjuntas e combinadas, do que é a minha experiência este será porventura o vetor menos desenvolvido e que pode traduzir-se numa fragilidade neste domínio das operações".*
E6	*"a criação de efeitos é efetuada na base do SCEPVA, e que está dependente dos países, no âmbito das suas capacidades e limitações legais"; "A principal vulnerabilidade que identifico na capacidade Ciber da NATO prende-se com a dependência que o Comandante Operacional tem do que os países possam ou não oferecer, conforme acima*

	referido. O adestramento é um aspeto muito relevante, daí a realização de exercícios. O acrónimo DOTMLPII contempla no "P" do pessoal/recursos humanos, os quais são cada vez mais relevantes nas nossas organizações"; "Num mundo cada vez mais globalizado, onde existem as interdependências, verifica-se muitas vezes a opção de se adquirirem serviços e o estabelecimento de contratos nesse sentido, em vez do desenvolvimento de capacidades próprias"; "a dificuldade na condução das operações uma vez que a criação de efeitos (SCEPVA) não está "debaixo" do Comandante Operacional, levando à necessidade de uma maior coordenação".
E7	*"A grande lacuna da NATO é interoperabilidade e partilha de conhecimento de conhecimento"; "ninguém quer partilhar como produz os efeitos no Ciberespaço"; "existe uma grande escassez de pessoal com as competências necessárias, o que é transversal a praticamente todos os países membros da NATO"; "Existem estudos para renovar sistemas legacy (desatualizados), que apontam a necessidade de despender biliões de dólares"; "relativamente a sistemas do tipo of-line, é necessário substituir biliões de software"; "Diria assim que o grande problema da NATO é a renovação dos seus equipamentos e a evolução tecnológica, que é muito difícil de acompanhar"; "possuem recursos limitados"; "Os países não prescindem dos seus recursos para disponibilizar à NATO porque estão totalmente dependentes deles para defender os seus sistemas"; "As nações não querem dar as suas capacidades, porque perdem as suas capacidades e revelam as suas próprias capacidades.*
E8	*"a dependência dos seus membros"; "para condução de operações destinadas a provocar efeitos através do mecanismo SCEPVA poderá constituir uma limitação durante a condução de operações no ciberespaço".*
E9	*"Se por um lado a Doutrina pode ser um ponto forte na NATO, é também uma limitação, uma vez que qualquer alteração ou desenvolvimento de nova Doutrina tem de ser aprovada pelos 30 Aliados"; "diferentes Nações se encontram em pontos de desenvolvimento, com investimentos completamente desfasados, em particular no que diz respeito à capacidade de desenvolver operações no ciberespaço. Adicionalmente, um dos aspetos em que é mais difícil obter concenso passa pelo desenvolvimento (ou utilização) de capacidades ofensivas no Ciberespaço pela NATO, que até este momento se encontra fora do horizonte"; "Até hoje, a NATO nunca financiou um programa comum destinado a desenvolver capacidades ofensivas (os investimentos da Aliança passam por capacidades não ofensivas, como ISR, transporte estratégico, AWACS, etc) "; "A capacidade da NATO para atuar no Ciberespaço, quer na componente de cibersegurança como de operações no ciberespaço, depende de recursos qualificados que, na maioria dos casos, provém das Nações"; "a NATO depende das contribuições dos Aliados para a condução de operações ofensivas".*
E10	*"Há também infraestruturas nacionais críticas dentro do JOA que pode afetar as operações da NATO, por exemplo, Sistemas SCADA que suportam um sistema de tecnologia de operações de infraestruturas vitais para a missão – que precisam ser defendidos"; "A NATO é uma aliança defensiva e não tem planos de desenvolver suas próprias capacidades ofensivas no ciberespaço"; "Observe que os Aliados manterão o controle de suas capacidades em todos os momentos quando forem usados durante as missões e operações da NATO".*
Pontos Fortes da Capacidade de Ciberdefesa Nacional	
E1	*"Podemos ajudar a desenvolver novos cursos, novas áreas nichos, que depois complementadas com as outras maiores aportem resultados"; "e validam-se competências essencialmente com treino"; "último domínio, aquilo que se que se pode designar por validador de competências"; "neste momento temos docentes nacionais a dar formação à escola da NATO"; "Relativamente à liderança as coisas estão a mudar"; "Esta capacidade vai ser uma capacidade articulada com a componente operacional do EMGFA, do Comando Operacional do EMGFA, e o Comando do EMGFA tem em cada um dos ramos uma antena sobre a qual vai exercer comando, porque é natural que seja".*
E2	*"disponibilização de oportunidades nacionais de formação e treino à NATO e aliados"; "a passagem do COCiber para a responsabilidade de coordenação do CCOM traduz o assumir do ciberespaço como um domínio de condução de operações e produção de efeitos. Desta forma, existirá uma segregação vantajosa e atribuição a entidades distintas das responsabilidades de identificação de requisitos operacional"; "desenvolvimento de capacidade para satisfação dos requisitos operacionais identificados"; "Como elemento de ligação ás entidades congéneres internacionais no âmbito da EU e NATO possibilita a partilha de informação e de experiencias de emprego de meios na produção de efeitos e de proteção das redes operacionais"; "o pessoal deverá estar treinado na componente de produção de efeitos por forma a poder vir a reforçar o COCiber".*
E3	*"houve um forte desenvolvimento doutrinal"; "também ao nível organizacional haverá mais aprovações. A liderança interna é um ponto forte da capacidade portuguesa"; "e também o treino"; "e a interoperabilidade eram também um dos pontos fortes da capacidade de Ciberdefesa das nossas Forças Armadas"; "A criação de uma Escola de Ciberdefesa teve como objetivo de alimentar num curto prazo aquilo que seria um Corpo, ou um Comando de Ciberdefesa Nacional, contudo penso que neste momento este vetor ainda não se constitua como um ponto forte, mas no futuro próximo poderá ser".*

E4	*"criação de um Comando de Operações de Ciberdefesa aparenta ser o mais adequado para os dias de hoje"; "capacidade de geração de recursos humanos"; "fortemente especializado"; "deve ser dada uma importância elevada ao recrutamento, seleção, retenção"; "capacitação da componente humana, sendo esta uma prioridade"; "tornar-nos em organizações com as mais avançadas tecnologias"; "trabalho desenvolvido na área das Tecnologias Emergentes e Disruptivas (EDT) nos dará mais conhecimento sobre o ciberespaço e a capacidade para nos tornarmos mais resilientes".*
E5	*"transformação de uma componente que se inseria numa vertente puramente tecnológica para uma capacidade desta feita também orientada para a componente operacional, criando ligações mais estreitas com a componente de operações conjuntas"; "com a participação nacional no maior exercício tecnológico de interoperabilidade da NATO, o CWIX (Coalition Warior Interoperability eXploration, eXperimentation, eXamination, eXercise) "; "Foi feita uma aposta para a criação de uma Escola de Ciberdefesa com a capacidade de formar pessoas especializadas nesta área da guerra, com vista à criação de um corpo de tropas tecnologicamente avançado*
E6	*os principais pontos fortes da capacidade de Ciberdefesa nacional são a Liderança"; "a Organização"; "a Interoperabilidade"; "A liderança, pois a DEEMGFA 2018-2021 tinha como uma das suas orientações estratégicas, a OE#2, o desenvolvimento da capacidade de ciberdefesa."; "Organização porque pôde ser edificada à luz de outras experiências internacionais, com as boas práticas aplicadas"; "existe uma ligação entre o EMGFA e os Ramos muita salutar nesta área. Interoperabilidade porque ao ser o EMGFA a adquirir todos os equipamentos para as Forças Armadas, numa situação de compromisso entre todos e no desenvolvimento comum de requisitos, não existem sistemas diferentes para fazer o mesmo"; "qualquer operador da marinha poderá operar o sistema do Exército ou da Força Aérea, pois são idênticos".*
E7	*"A base de qualquer capacidade é a escola, e neste momento está em funcionamento, pelo que me parece o nosso ponto mais forte"; "A criação do Comando de Ciberdefesa foi um passo importante para a edificação da capacidade, aproxima-nos mais do CEMGFA, e pode ajudar facilitar o processo de decisão".*
E8	*"tem existido a preocupação em elaborar doutrina sobre o assunto, designadamente a Publicação de Doutrina Militar Conjunta (PDMC) 3.20 - Operações no Ciberespaço"; "A recente criação do COCiber que prevê o aumento dos efetivos atribuídos a esta capacidade para efeitos de planeamento e condução de operações no ciberespaço"; "A recente criação do COCiber que prevê o aumento dos efetivos atribuídos a esta capacidade para efeitos de planeamento e condução de operações no ciberespaço"; "aquisição de dispositivos de segurança (e.g. Firewalls) e fermentadas de segurança (e.g. SIEM, entre outros) ao abrigo da Lei de Programação Militar (LPM), que têm sido disponibilizados ao Centro de Ciberdefesa e CIRC dos Ramos"; "Com a publicação da nova Lei Orgânica do EMGFA ficou claramente estabelecida a competência funcional e técnica do COCiber em relação aos Ramos"; "A Publicação de Doutrina Militar Conjunta (PDMC) 3.20 - Operações no Ciberespaço, em aprovação, irá ajudar a clarificar as relações de Comando entre as diversas entidades envolvidas nas operações no ciberespaço"; "os dispositivos de segurança e as ferramentas de segurança têm sido adquiridas centralmente pelo EMGFA"; "tem sido tida em consideração a interoperabilidade entre o CCD e os CIRC dos Ramos"; "a criação da Escola de Ciberdefesa destinada a formar os elementos nacionais com as qualificações necessárias para a condução de todos os tipos de operações no ciberespaço"; "com o aumento de pessoal será possível ao COCiber incrementar a sua capacidade de monitorização do ciberespaço".*
E9	*"criação de carreiras específicas para esta valência"; "criação de carreiras específicas para esta valência"; "Treino (ainda antes da realização de investimentos em Material ou Infraestruturas)"; "identificação de uma Liderança que consiga efetuar a ligação entre os objetivos estratégicos para a capacidade e os recursos disponíveis".*
E10	*"embora eu tenha ficado muito impressionado com a ferramenta PRT Situational Awareness quando ela foi usada no CWIX".*
Vulnerabilidades da Capacidade de Ciberdefesa Nacional	
E1	*"Mas depois falta-nos um ou outro, que é aquele que fecha o ciclo, que é a validação de competências"; "Nós temos que ter ajustado, neste ecossistema, uma forma de validar competências"; "temos que apostar primeiro na primeira leva de formadores, temos que aperfeiçoar muito a sua formação, e estes indivíduos vão ser um multiplicador da formação"; "temos que apostar primeiro na primeira leva de formadores, temos que aperfeiçoar muito a sua formação, e estes indivíduos vão ser um multiplicador da formação"; "O vetor humano, é o principal"; "é essencialmente o investimento tecnológico".*
E2	*"Apesar da responsabilidade de edificação de capacidade de ciberdefesa (incluindo treino e exercícios) continuar na dependência funcional e técnica de uma entidade de cariz tecnológico (o Centro de Comunicações e Informação, Ciberespaço e Espaço, CCICE) "; "o Comandante do Comando de Operações de Ciberdefesa (COCiber) se encontrar na directa dependencia do CCICEVO reforço da capacidade por parte dos Ramos, designadamente em estados de guerra e de excepção, pode materializar uma vunerabilidade quando os Ramos não conseguirem competir por recrutamento e retenção de recursos"; "Face á especificidade das redes e sistemas existentes nos diferentes Ramos é de extrema importância que sejam garantidas as capacidades próprias de monitorização, deteção, proteção, defesa, resposta e recuperação"; "é o vetor Pessoal";*

	"Especialistas no area ciber são escassos e cobiçados por diferentes setores nacionais"; "Infelizmente as Forças Armadas não conseguem competir com o setor privado em termos de vencimentos e regalias para estes recursos, assim torna-se extremamente difícil recrutar e reter recursos, civis e militares".
E3	*"assim como é para Portugal"; "deveria haver mais envolvimento Nacional com a NCIA" A principal vulnerabilidade prende-se com a falta de pessoal qualificado"; "e que se tornam uma vulnerabilidade, que são os equipamentos"; "e as infraestruturas, mas também o treino, que muitas vezes é condicionado pelas restrições financeiras associadas às necessidades de deslocamento e alojamento fora do país".*
E4	*"capacidade de geração e retenção de recursos humanos"; "domínio de capital intelectual intensivo"; "mitigar esta eventual dificuldade será através da formação destes recursos humanos"; "assegurando-lhes a respetiva progressão na carreira".*
E5	*"capacidade ainda está em edificação"; "a nossa principal vulnerabilidade neste estágio do desenvolvimento é o vetor do Pessoal"; "escassez de recursos com as capacidades tecnológicas que são necessárias aos ciber-guerreiros, bem como os que existem são de difícil retenção nos quadros das FFAA face ao valor que representam no mercado de trabalho civil"; "pouca atratividade da carreira militar"; "intenção de criação do corpo mantém-se recorrendo a militares de carreira com especializações em componentes da guerra no ciberespaço".*
E6	*"e as infraestruturas, mas também o treino, que muitas vezes é condicionado pelas restrições financeiras associadas às necessidades de deslocamento e alojamento fora do país"; "Importa uma resposta integrada nacional às ameaças onde é fundamental a coordenação Nacional, e aqui o G4, que integra o CCD, CNCS, UNC3T e SIS, tem um papel relevante".*
E7	*"As grandes vulnerabilidades da capacidade prendem-se com a liderança versos vontade de desenvolver a capacidade"; "As grandes vulnerabilidades da capacidade prendem-se com a liderança versos vontade de desenvolver a capacidade".*
E8	*"é o caso de Portugal onde a componente financeira não permite concorrer com o setor privado"; "torna-se necessário elaborar um conjunto de Normas de Execução Permanente (NEP) ao nível do Comando de Operações de Ciberdefesa (COCiber) de modo a regular determinados processos no âmbito desta capacidade"; "eventuais conflitos de liderança em relação ao COCiber uma vez que este depende hierarquicamente do CCICE, porém para efeitos de condução de operações no ciberespaço poderá estar na dependência do CCOM"; "eventuais conflitos de liderança em relação ao COCiber uma vez que este depende hierarquicamente do CCICE, porém para efeitos de condução de operações no ciberespaço poderá estar na dependência do CCOM"; "existem atualmente constrangimentos relativos ao recrutamento e retenção de recursos humanos para esta área"; "rapidamente os espaços atribuídos irão ficar aquém das necessidades para comportar todo este pessoal"; "necessidade de edificação da Escola da Ciberdefesa com as condições necessárias para o cumprimento da sua missão"; "Treino"; "o Pessoal"; "Ao nível do Treino importa garantir a assinatura do contrato com a entidade Israelita selecionada para ministrar formação na Escola de Ciberdefesa, de modo a incrementar o grau de preparação dos formandos, nomeadamente para condução de operações CISRO e OCO. "; "tem se verificado alguma dificuldade em recrutar pessoal para o CCD"; "qualificação do pessoal, pois considerando que esta é uma área com bastante procura no mercado de trabalho será necessário criar condições atrativas de modo a conseguir reter o pessoal".*
E9	*"escassez de recursos humanos"; "existe uma falta reconhecida em pessoal qualificado para o planeamento e execução de operações no ciberespaço. O tipo de conhecimento necessário e o investimento que é necessário realizar na qualificação e especialização desses elementos (com a profundidade requerida) talvez encontre apenas paralelo (nas Forças Armadas Portuguesas) em carreiras como a de piloto aviador"; "é necessário ter uma liderança com uma visão assertiva de qual o nível de ambição que se pretende ter para um Comando de Operações no ciberespaço, e o que é possível implementar e em que prazos".*
Contributo nacional para a Ciberdefesa da NATO	
E1	*"Nós estamos é nos sítios certos, porque conseguimos antecipar onde é que a capacidade vai buscar o centro de gravidade, e como nos antecipámos estamos no "mainstream", onde estamos a fornecer serviços neste domínio aos outros países com potencial para o fazer".*
E2	*"passam a contar nas suas fileiras com pessoal com experiência de atuação nesta componente defensiva"; "Os compromissos assumidos por Portugal para a edificação de capacidades, mais especificamente no âmbito do NATO Cyber Pledge, contemplavam para o Exército um conjunto de módulos táticos de ciberdefesa para garantirem a monitorização, deteção, proteção, defesa, resposta e recuperação das redes de comunicações e sistemas de informação táticos das unidades disponibilizadas à NATO"; "Constituir-se-à como mais um meio de coleta, interpretação, divulgação e partilha de informação relativa a riscos, ameaças e formas de mitigação de vulnerabilidades"; "Se for identificado por Portugal o nível de ambição e reunidas todas as condições (pessoal, material, financeiro) para o desenvolvimento de uma capacidade de produção*

	de efeitos (operações ofensivas) no ciberespaço suficientemente robusta e tecnologicamente avançada, guarnecida com pessoal devidamente formado e treinada poderemos eventualmente ser o oitavo país a disponibilizar-se para conduzir efeitos em nome da NATO".
E3	*"O reforço da parte do pessoal é sem dúvida o grande contributo que Portugal pode fornecer à NATO"; "Penso que deve também haver uma forte aposta na capacidade Ofensiva"; "em pessoal com esta capacidade ofensiva, particularmente na capacidade ISR".*
E4	*"Educação Treino e Exercícios Cyber"; "edificação do Cyber Academia and Innovation Hub"; "à Escola de Ciberedefesa"; "Pessoas, com as respetivas competências"; "a capacidade e processos, incorporando iniciativas de segurança e privacidade"; "a Tecnologia, com capacidades de ciberdefesa e cibersegurança"; "Automação, que permita a monitorização em tempo real da eficácia dos controlos"; "A edificação de uma entidade formadora conjunta"; "ligação à comunidade académica e empresarial nacional e estimular o conhecimento dos cidadãos sobre a missão da ciberdefesa"; "articular-se com o Cyber Academia and Innovation Hub (CAIH) "; "capacitação de recursos humanos na área da cibersegurança, nacionais e internacionais, contribuindo com os seus conhecimentos específicos para a capacitação tecnológica dos recursos humanos das entidades com responsabilidade na segurança do ciberespaço".*
E5	*"a edificação têm-se centrado no desenvolvimento de capacidades de defesa própria para ataques que possam afetar as redes nacionais"; "a liderança da área funcional da Ciberdefesa, considero que as FFAA portuguesas têm dado um contributo bastante forte na componente de treino da Aliança".*
E6	*"o principal contributo que Portugal pode oferecer à NATO consiste na criação de efeitos"; "disponibilidade de pessoal com know how para cargos na estrutura da Aliança".*
E7	*"participar nos exercícios NATO, no sentido de desenvolver as nossas TTP"o principal contributo que Portugal pode oferecer à NATO consiste na criação de efeitos"; "disponibilidade de pessoal com know how para cargos nas estrutura da Aliança".interoperabilidade"o principal contributo que Portugal pode oferecer à NATO consiste na criação de efeitos"; "disponibilidade de pessoal com know how para cargos nas estrutura da Aliança"; "aprender os que os outros estão a fazer".*
E8	*"através do vetor do Treino"; Portugal ao obter capacidade para desenvolver Defensive Cyberspace Operations (ODO), Cyberspace Intelligence, Surveillance and Reconnaissance Operations (CISRO) e Offensive Cyberspace Operations (OCO) também permitirá à NATO beneficiar desta capacidade, através do mecanismo SCEPVA"; "Também o vetor de Pessoal contribuirá para o reforço da capacidade".*
E9	*"o preenchimento de posições abertas nos diversos órgãos relacionados com o ciberespaço na estrutura da NATO, assim como a capacitação desses recursos para que possam executar a sua missão, é sem dúvida um dos principais vetores em que a capacidade de Ciberdefesa nacional pode contribuir para a capacidade da NATO"; "Dessa forma, o potencial desenvolvimento de uma capacidade ofensiva na capacidade de Ciberdefesa nacional e a sua disponibilização à NATO sob esse mecanismo poderia ser uma perspetiva importante para o reforço da capacidade da NATO".*
E10	*"Compartilhamento de Consciência Situacional do Ciberespaço"; "Cooperação das Equipes de Reação Rápida"; "Compartilhamento de inteligência cibernética"; "Formação Coletiva - Cyber Perseu?"; "Treinamento Individual"; "Treinamento Individual"; "Os exercícios de unidades cibernéticas nacionais podem refletir como operar sob uma infraestrutura de rede da OTAN"; "Capture dados para análise".*

Apêndice F — Categorias e Subcategorias

Quadro 5 - Categorias e subcategorias

Categorias					
Características do Ciberespaço		Implicações do Ciberespaço	Desafios e oportunidades do Ciberespaço		Relevância do Ciberespaço
Subcategorias					
Acessibilidade Ambiente de informação Ameaça constante Anonimato Assimetria Complexidade Componente física Componente virtual Construção humana Dependência	Difícil regulamentação Dissuasão Global Multidimensionalidade Responsabilidade Sem fronteiras Tempo e velocidade Transversalidade Visibilidade	Ambiente informacional Complexidade Comunicação e C2 Desinformação Economia *Enablers* operacionais Impacto domínios tradicionais Infraestruturas e serviços críticos Planeamento Regulamentação Segurança das informações Tomada de decisão	**Desafios:** Ameaças Assimetria Autonomia Coordenação Dependência Diferenças culturais Doutrina Gestão da informação Mistificação Regulamentação Segurança Sensibilização Velocidade da difusão	**Oportunidades:** Desenvolvimento económico Desenvolvimento tecnológico Globalização Informação e conhecimento Interconectividade	Artº 5º Dependência Independência Transversalidade Novas capacidades Política Segurança

Categorias						
Possibilidades e limitação NATO		Possibilidades e limitações Ciberdefesa NATO		Possibilidades e limitações Ciberdefesa Nacional		Contributo nacional para a NATO
Subcategorias						
Possibilidades Conhecimento Dissuasão Domínio operacional Impacto moderado Sincronização das operações	**Desafios** Ambiente competitivo Ameaça Coordenação operações Dependência Domínio operacional Infraestruturas Segurança Treino	**Pontes fortes NATO** Doutrina Organização Treino Material Liderança Pessoal Infraestruturas Interoperabilidade	**Pontos fracos NATO** Doutrina Organização Treino Material Liderança Pessoal Infraestruturas Interoperabilidade	**Pontos fortes nacionais** Doutrina Organização Treino Material Liderança Pessoal Infraestruturas Interoperabilidade	**Pontos fracos nacionais** Doutrina Organização Treino Material Liderança Pessoal Infraestruturas Interoperabilidade	Defesa das redes nacionais Fornecimento de serviços Interoperabilidade Operações ofensivas Pessoal especializado Treino

Apêndice G — Livro de Códigos do *NVivo*

Quadro 6 - Livro de Códigos do *NVivo*

Categoria/Subcategoria	N.º de Sujeitos	N.º de Referências	Categoria/Subcategoria	N.º de Sujeitos	N.º de Referências
Características do Ciberespaço	**10**	**114**			
Acessibilidade	1	1	Anonimato	3	4
Ameaça constante	3	6	Complexidade	5	5
Assimetria	3	4	Componente virtual	8	15
Componente física	7	10	Dependência	4	5
Construção humana	2	2	Dissuasão	1	1
Difícil regulamentação	4	11	Multidimensionalidade	1	4
Global	1	1	Sem fronteiras	6	10
Responsabilidade	3	5	Transversalidade	5	13
Tempo e velocidade	6	8	Visibilidade	1	1
Ambiente de informação	4	8			
Implicações do Ciberespaço	**10**	**48**			
Ambiente informacional	2	3	Impacto nos domínios tradicionais	5	13
Complexidade	1	1	Infraestruturas e serviços críticos	2	2
Comunicação e C2	5	9	Planeamento	1	1
Desinformação	3	3	Regulamentação	2	5
Economia	1	1	Segurança das informações	4	7
Enablers operacionais	2	2	Tomada de decisão	1	1
Desafios e oportunidades do Ciberespaço	**10**	**82**			
Desafios ciberespaço	10	54	Doutrina	1	2
Ameaças	4	7	Gestão da informação	3	9
Assimetria	3	4	Mistificação	1	1
Autonomia	1	1	Regulamentação	5	6
Coordenação	1	2	Segurança	3	12
Dependência	5	7	Sensibilização	1	1
Diferenças culturais	1	1			
Relevância do Ciberespaço	**8**	**32**			
Artº 5º	1	1	Novas capacidades	4	7
Dependência	2	2	Política	3	3
Independência	2	2	Segurança	6	10

Transversalidade	3	7			
Possibilidades e limitação NATO	**9**	**24**			
Possibilidades NATO:	6	13	Limitações NATO:	8	14
Conhecimento	3	4	Ambiente competitivo	1	1
Dissuasão	1	1	Ameaça	1	1
Domínio operacional	3	4	Coordenação de operações	2	2
Impacto moderado	2	3	Dependência	1	1
Sincronização das operações	1	1	Domínio operacional	1	1
			Infraestruturas	1	2
			Segurança	1	1
			Treino	1	2
Possibilidades e limitações Ciberdefesa NATO	**10**	**110**			
Pontes fortes NATO:	9	54	Pontos fracos NATO:	10	56
Doutrina	6	11	Doutrina	8	119
Organização	7	9	Organização	3	5
Treino	6	10	Treino	2	2
Material	4	4	Material	3	5
Liderança	1	1	Liderança	1	1
Pessoal	3	9	Pessoal	6	9
Infraestruturas	3	3	Infraestruturas	1	1
Interoperabilidade	4	7	Interoperabilidade	7	14
Possibilidades e limitações Ciberdefesa Nacional	**10**	**102**			
Pontos fortes nacionais:	10	53	Pontos fracos nacionais:	9	49
Doutrina	3	3	Doutrina	1	1
Organização	7	10	Organização	2	2
Treino	7	11	Treino	5	9
Material	4	5	Material	2	2
Liderança	5	7	Liderança	3	4
Pessoal	4	8	Pessoal	7	23
Infraestruturas	0	0	Infraestruturas	2	3
Interoperabilidade	5	9	Interoperabilidade	4	5
Contributo nacional para a NATO	**10**	**40**			
Defesa redes nacionais	3	5	Operações ofensivas	5	5
Fornecimento de serviços	2	2	Pessoal especializado	5	7
Interoperabilidade	4	7			