INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR DA FORÇA AÉREA

2021/2022

TII

DESENVOLVIMENTO DA CAPACIDADE DE CIBERDEFESA DESTACÁVEL (NATO CD-DEPLOY)

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

Rui Pedro Alves Pereira

CAP/TINF

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

DESENVOLVIMENTO DA CAPACIDADE DE CIBERDEFESA DESTACÁVEL (NATO CD-DEPLOY)

CAP/TINF Rui Pedro Alves Pereira

Trabalho de Investigação Individual CPOS-FA 2021/22 2.ª Ed.

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

DESENVOLVIMENTO DA CAPACIDADE DE CIBERDEFESA DESTACÁVEL (NATO CD-DEPLOY)

CAP/TINF Rui Pedro Alves Pereira

Trabalho de Investigação Individual CPOS-FA 2021/22 2.ª Ed.

Orientador: MAJ/TINF Carlos Eduardo Passos

Pedrouços 2022

Declaração de compromisso Antiplágio

Eu, **Rui Pedro Alves Pereira**, declaro por minha honra que o documento intitulado **Desenvolvimento da capacidade de Ciberdefesa Destacável (NATO CD-DEPLOY)** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Promoção a Oficial Superior – Força Aérea 2021/2022 2.ª Edição** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.
Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 12** de **julho** de **2022**

Rui Pedro Aves Pereira

CAP/TINF

Agradecimentos

As primeiras palavras de agradecimento dirijo-as, como não podia deixar de ser, à minha esposa, Ana Pereira, que uma vez mais, como várias e de forma contínua, me tem suportado sempre que a exigência da vida profissional extravasa para aquilo que devia ser o tempo pessoal. Desde sempre que me lembro de estares lá, para me apoiar e ajudar, e sei que enquanto estiveres comigo, tudo irá correr bem.

De seguida agradeço à minha família e amigos, em particular aos meus filhos, e peço desculpa se tive menos disponibilidade do que devia.

Em segundo lugar agradeço aos meus camaradas, os de curso e os restantes, que me ajudaram, fosse no trabalho e no estudo, fosse a lembrar que há outras coisas importantes na vida além do trabalho e do estudo. Ajudaram-me de forma inestimável a perceber o posicionamento da "linha de ambição".

Finalmente agradeço ao meu orientador Major Passos, por organizar e direcionar o meu esforço, e ao Tenente-Coronel Vinagreiro, por ter facilitado informação crucial para o desenvolvimento deste estudo, e pela forma "terra-a-terra" como conseguiu passar-me os fundamentais deste estudo.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A importância da ciberdefesa, tanto a nível nacional e internacional, tem assumido um destaque, de tal forma que a NATO desenvolveu o conceito de ciberdefesa destacável, para aplicação em forças destacadas com sistemas de informação e comunicações, o NATO CD-DEPLOY.

Este estudo tem como objetivo propor medidas para a implementação da capacidade ciberdefesa destacável nas FFAA Portuguesas, NATO CD-DEPLOY. Foi desenvolvido segundo uma investigação de raciocínio indutivo, assente numa estratégia mista, baseada em análise documental e entrevistas semiestruturadas.

Os resultados obtidos permitiram a identificação de cinco medidas que contribuem para a certificação das FFAA Portuguesas na capacidade de ciberdefesa destacável, NATO CD-DEPLOY, proporcionando uma melhor proteção às nossas forças militares destacadas. Destas medidas de implementação, destaca-se a retoma rápida da participação em exercícios nacionais e internacionais de cariz ou com uma componente ciber, a aquisição de um Sistema de *data labelling and binding*, e concluir o treino dos elementos que vão operar as plataformas de *Online Computer Forensic* e *Online Vulnerability Assessment*.

Palavras-chave:

Ciberdefesa; ciberdefesa destacável; cibersegurança; NATO CD-DEPLOY.

Abstract

The relevance of Cyber defence, both national and international, has grown in such a way, that NATO has developed the deployable cyber defence concept, to be used by deployed forces with communications and informations systems.

This study aims to propose measures for the implementation of deployable cyber defence capability in the Portuguese Armed Forces, NATO CD-DEPLOY. It was developed according to an inductive reasoning research, with a mixed strategy, based on documental analysis and semi-structured interviews.

The results obtained allowed the identification of five measures that contribute to the certification of the Portuguese Armed Forces in the deployable cyber defense capability, NATO CD-DEPLOY, providing better protection to our deployed military forces. Of these implementation measures, taking part briefly in national or international cyber exercises, or with a cyber componente, the acquisition of a data labeling and binding system and completion of the training of the elements that will operate the Online platforms Computer Forensic and Online Vulnerability Assessment should be highlighted.

Keywords:

Cyber defence; d*eployable cyber defence*; c*yber security*; NATO CD-DEPLOY.

Lista de abreviaturas, siglas e acrónimos

AR	Assembleia da República
AJP	*Allied Joint Publication*
AR	Assembleia da República
C2	Comando e controlo
CACLA	Centro de Avaliação, Certificação e Lições Aprendidas
CAIH	*Cyber Academia and Innovation Hub*
CC	*Capability Codes*
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CCICE	Centro de Comunicações e Informação, Ciberespaço e Espaço
CCOM	Comando Conjunto para as Operações Militares
CC&S	*Capability Codes and Capability Statements*
CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CIS	*Communications and Information Systems*
CISIO	*Communication and Information Systems Infrastructure Operations*
CISRO	*Cyberspace Intelligence, Surveillance and Reconnaissance Operation*
CNCS	Centro Nacional de Cibersegurança
COCiber	Comando de Operações de Ciberdefesa
COVID-19	*Coronavirus disease* 2019
DCO	*Defensive Cyberspace Operations*
ECCiber	Equipa de Combate no Ciberespaço
ECD	Escola de Ciberdefesa
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EMGFA	Estado Maior General Forças Armadas
EPCiber	Equipa de Proteção do Ciberespaço
ERCiber	Equipa de Resposta no Ciberespaço
FFAA	Forças Armadas
FMCiber	Forças de Missão do Ciberespaço
FMN	*Federated Mission Network*
FOCiber	Força de Operações de Ciberdefesa

GP	Governo de Portugal
IDM	*Internal Defensive Measures*
JCS	*Joint Chiefs of Staff*
JFC	*Joint Force Commander*
LOEMGFA	Lei Orgânica do Estado-Maior-General das Forças Armadas
LPM	Lei de Programação Militar
MI	Medida para implementação
NATO	North Atlantic Treaty Organization
NCIA	NATO *Communication and Information Agency*
NDPP	NATO Defence Planning Process
OCO	*Offensive Cyberspace Operations*
OE	Objetivo Específico
OPCON	Controlo Operacional
OG	Objetivo Geral
PDMC	Publicação Doutrina Militar Conjunta
RA	*Response Actions*
RDN	Redes da Defesa Nacional
SCEPVA	*Sovereign Cyber Effects Provided Voluntarily by Allies*
SRSIC	Sub-Repartição de Segurança Informática e Ciberdefesa
QC	Questão Central
QD	Questão Derivada
TACON	Controlo Tático
TII	Trabalho de Investigação Individual
UE	União Europeia

1. Introdução

O Conceito estratégico da *North Atlantic Treaty Organization* (NATO) identifica três tarefas essenciais e pilares da Aliança: a defesa coletiva, gestão e resposta a crises, e segurança cooperativa (North Atlantic Treaty Organization [NATO], 2010).

Na cimeira de Gales, 2014, a NATO estabeleceu que a ciberdefesa constitui parte integrante das funções essenciais de defesa coletiva da Aliança, indicando que a perigosidade e frequência de ataques cibernéticos vai aumentar, podendo chegar ao limite de ameaçar a segurança e estabilidade nacional e euro-atlântica (NATO, 2014). Nesta mesma cimeira, foi realçado que a responsabilidade primária da NATO em matéria de ciberdefesa é a defesa das suas redes e sistemas, destacando que as nações Aliadas têm que desenvolver capacidades para defender as suas redes e sistemas. (NATO, 2014).

No *Cyber Defense Pledge* da Cimeira de Varsóvia em 2016, a NATO identifica a intenção de se conseguir defender no ciberespaço como em qualquer das outras componentes, aérea, marítima ou terrestre, reconhecendo formalmente o ciberespaço como um novo domínio operacional (NATO, 2016b). Neste compromisso solene, a NATO declara a intenção de garantir uma Aliança treinada, segura e consciente do ambiente cibernético, e integrando a ciberdefesa nas operações e em redes projetáveis (NATO, 2016b).

De forma a desenvolver as capacidades da ciberdefesa na NATO, foram determinados objetivos para capacidades de ciberdefesa nacional dos Aliados por via do *NATO Defence Planning Process* (NDPP), que materializa estes objetivos em Requisitos Mínimos de Capacidades (*Minimum Capability Requirements*) (NATO, 2021).

A nível nacional foram estabelecidos os enquadramentos estruturais. Está plasmada no Conceito Estratégico de Defesa Nacional (CEDN) a intenção de edificar a capacidade de Ciberdefesa Nacional, identificando os ataques cibernéticos como ameaça crescente, complexa e com um potencial devastador, e atribui às Forças Armadas a incumbência de erigir a capacidade de Ciberdefesa Nacional como resposta a este tipo de ameaça (Resolução de Conselho de Ministros n.º 19/2013 de 21 de março, 2013). Concomitantemente, a Lei de Programação Militar (LPM) prevê um orçamento crescente para esta atividade, tendo a Programação do investimento público das Forças Armadas em matéria de armamento e equipamento um total de 11.800.000€ para o quadriénio de 2019 a 2022 e 18.100.000€ para o quadriénio de 2023 a 2026, sinal do empenho orçamental crescente nesta atividade (Lei Orgânica n.º 2/2019 de 17 de junho, 2019).

A Diretiva Estratégica do Estado-Maior-General das Forças Armadas (EMGFA) 2018/2021 pretende "[…] dotar as Forças Armadas com capacidade acrescida para defender as redes militares contra ciberataques e realizar operações militares no ciberespaço" (Estado-Maior-General das Forças Armadas [EMGFA], 2018, p.22).

A Lei Orgânica do Estado-Maior-General das Forças Armadas (LOEMGFA), promulgada em janeiro de 2022, reflete as preocupações da NATO em matéria de ciberdefesa e é o culminar das iniciativas nacionais anteriormente referidas, instituindo o Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE), reconhecendo os novos domínios das operações - Espaço e Ciberespaço, colocado na direta dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), como forma de garantir a geração e operação de capacidades de resposta na salvaguarda da soberania e interesses nacionais (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022).

A Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023 identifica diferentes tipologias, agentes e motivações para as várias ameaças do ciberespaço nacional (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019). Identifica também que o crescente número de recursos de aprendizagem e ferramentas de fácil utilização, em conjunção com várias vulnerabilidades existentes no ciberespaço nacional, tem feito crescer o número de ataques no ciberespaço, e como forma de combater esta tendência, estabelece 6 eixos de atuação, que permitem cobrir os vários aspetos relacionados com a proteção do ciberespaço nacional (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019):

A ENSC pretende incrementar simultaneamente as capacidades do Centro Nacional de Cibersegurança (CNCS) e das FFAA, como forma de robustecer a cibersegurança e a ciberdefesa nacional, e estabelecer uma relação de cooperação que permita o uso dual destas capacidades e a partilha de informação aos vários níveis de decisão (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019).

Em linha com esta preocupação crescente com a proteção do ciberespaço, é pertinente a realização de um estudo sobre a implementação deste tipo de proteção para forças militares destacadas (J.M. Vinagreiro, entrevista por *email*, 11 de julho de 2022).

O objeto da investigação deste trabalho é a implementação da capacidade de ciberdefesa destacável nas FFAA Portuguesas, NATO CD-DEPLOY (NATO, 2016a).

A investigação será delimitada, à luz do preconizado por Santos e Lima (Santos & Lima, 2019, p. 42), nos seguintes âmbitos:

- Espacial, centrando-se nos órgãos e entidades das FFAA com responsabilidade especifica na ciberdefesa nacional;
- Temporal, reportando-se ao período de novembro de 2010 a julho de 2022;
- Conteúdo, referindo-se às capacidades de ciberdefesa das FFAA.

Estabelecido este enquadramento, o presente estudo tem como objetivo geral (OG) *Propor medidas que permitam que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY)*. Para este OG concorrem os seguintes objetivos específicos (OE):

OE1: Analisar a capacidade de ciberdefesa destacável NATO CD-DEPLOY.

OE2: Analisar as capacidades das FFAA Portuguesas em matéria de ciberdefesa.

Destes objetivos derivam a Questão Central (QC) de investigação, *Que medidas devem ser implementadas que permitam que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY)?*, da qual se deduzem as seguintes Questões Derivadas(QD):

QD1: Quais os requisitos para a capacidade de ciberdefesa destacável NATO CD-DEPLOY?

QD2: Quais as capacidades das FFAA Portuguesas em matéria de ciberdefesa?

Este documento está estruturado em cinco capítulos, sendo este a introdução. O segundo capítulo apresenta os conceitos teóricos mais relevantes para a compreensão deste trabalho, enquadrado pelos conceitos estruturantes, bem como o modelo de análise que orientou esta investigação. O terceiro capítulo descreve a metodologia e o método usados para a recolha de informação, que é apresentada no quarto capítulo, juntamente com a discussão dos resultados e as respostas obtidas às questões de investigação. No quinto capítulo são apresentadas as conclusões deste trabalho, as limitações, recomendações, e propostas de estudos futuros.

2. Enquadramento teórico e conceptual

Neste capítulo são introduzidos os conceitos mais relevantes para o entendimento deste trabalho de investigação.

Nota de autor:

Alguns termos usados nesta temática são usados em diferentes contextos, nomeadamente o uso da expressão ciber, que pode ser definida como um termo que conota uma relação com as tecnologias de informação (Schmitt, 2017). Os termos cibercrime, ciberespionagem, ciberguerra referem-se a atividades executadas com recurso ou através de meios ciber. Neste contexto, as expressões ciberataque, ataque cibernético, ataque ciber ou ataque no ciberespaço, são equivalentes, e referem-se a um ataque realizado através das tecnologias de informação no ciberespaço, tendo como alvo um ou mais sistemas, e como objetivo causar danos à segurança das tecnologias de informação e da comunicação, no que respeita à confidencialidade, integridade e disponibilidade (Schmitt, 2017).

O autor optou por manter as siglas dos termos mais comuns em inglês, ficando desta forma alinhado com a doutrina NATO, *Joint Chiefs of Staff* (JCS), União Europeia, e outras, e a própria doutrina nacional, emanada do EMGFA.

2.1 Revisão da literatura e conceitos estruturantes

Neste ponto explana-se o estado da arte enquadrado pelos conceitos estruturantes.

2.1.1 Ciberdefesa

A União Europeia (UE), no *EU Concept on Cyber Defence for EU-led Military Operations and Missions*, define ciberdefesa como a dimensão militar da cibersegurança, mas integrando tanto a perspetiva militar como civil (EUMS, 2016). A ciberdefesa inclui todas as medidas, técnicas e não técnicas que aumentam a resiliência dos Sistemas de Informação e Comunicação (*Communications and Information Systems* CIS) que suportam a defesa e os interesses nacionais (EUMS, 2016).

A ENSC define ciberdefesa como a "atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço." (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2889). Embora esta definição não seja muito profunda, e haja uma grande diversidade de definições, a ENSC estabelece que a ciberdefesa assenta em 3 vetores (Jesus, 2021):

- Defesa e proteção dos CIS da Defesa Nacional, por forma a garantir a continuidade das suas atividades;
- Exploração do ciberespaço, seja para recolha de informações ou para defesa do mesmo, incluindo capacidades ofensivas ou criação de efeitos que permitam a manutenção da iniciativa;
- Cooperação entre várias entidades, nacionais e internacionais, para haver uma capacidade de resposta, consolidada e integrada.

Em linha com estes vetores, no site da Defesa Nacional, na secção de Ciberdefesa, consta a seguinte informação: "As atividades de ciberdefesa constituem uma nova área do domínio das operações da Defesa Nacional e um contributo fundamental para a segurança do ciberespaço de interesse nacional. Na ciberdefesa incluem-se as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional, competindo esta missão às Forças Armadas." (Defesa Nacional, 2022a).

2.1.1.1 Ciberespaço

A definição nacional constante na ENSC diz que o "Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação." (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2889).

A NATO define o ciberespaço como um ambiente computorizado, construído de forma artificial, constantemente em mudança, assente numa infraestrutura que está interligada de forma global, que pode ser usado por qualquer pessoa ou organização e para qualquer fim (NATO, 2020).

O ciberespaço pode ser estruturado em três camadas, física, lógica e *ciber-persona*, como se pode ver na figura 1 (Joint Chiefs of Staff , 2018). A camada física contém toda a infraestrutura que interliga computadores, servidores e outros equipamentos que processam, transmitem e guardam dados, os meios de transmissão de dados, bem como sistemas eletrónicos, sensores, sistemas de armas e de Comando e Controlo (C2) (NATO, 2020).

A camada lógica é composta por código, que constitui sistemas operativos, aplicações, protocolos, *firmware*, bases de dados, entre outros. A camada lógica depende da camada física para funcionar (NATO, 2020).

A camada *ciber-persona* consiste em representações de identidades de pessoas ou organizações, como um *email*, um nome de utilizador ou um número identificativo de uma

pessoa ou organização. A camada *ciber-persona* depende da camada lógica e da camada física para poder ter acesso ao ciberespaço (NATO, 2020).

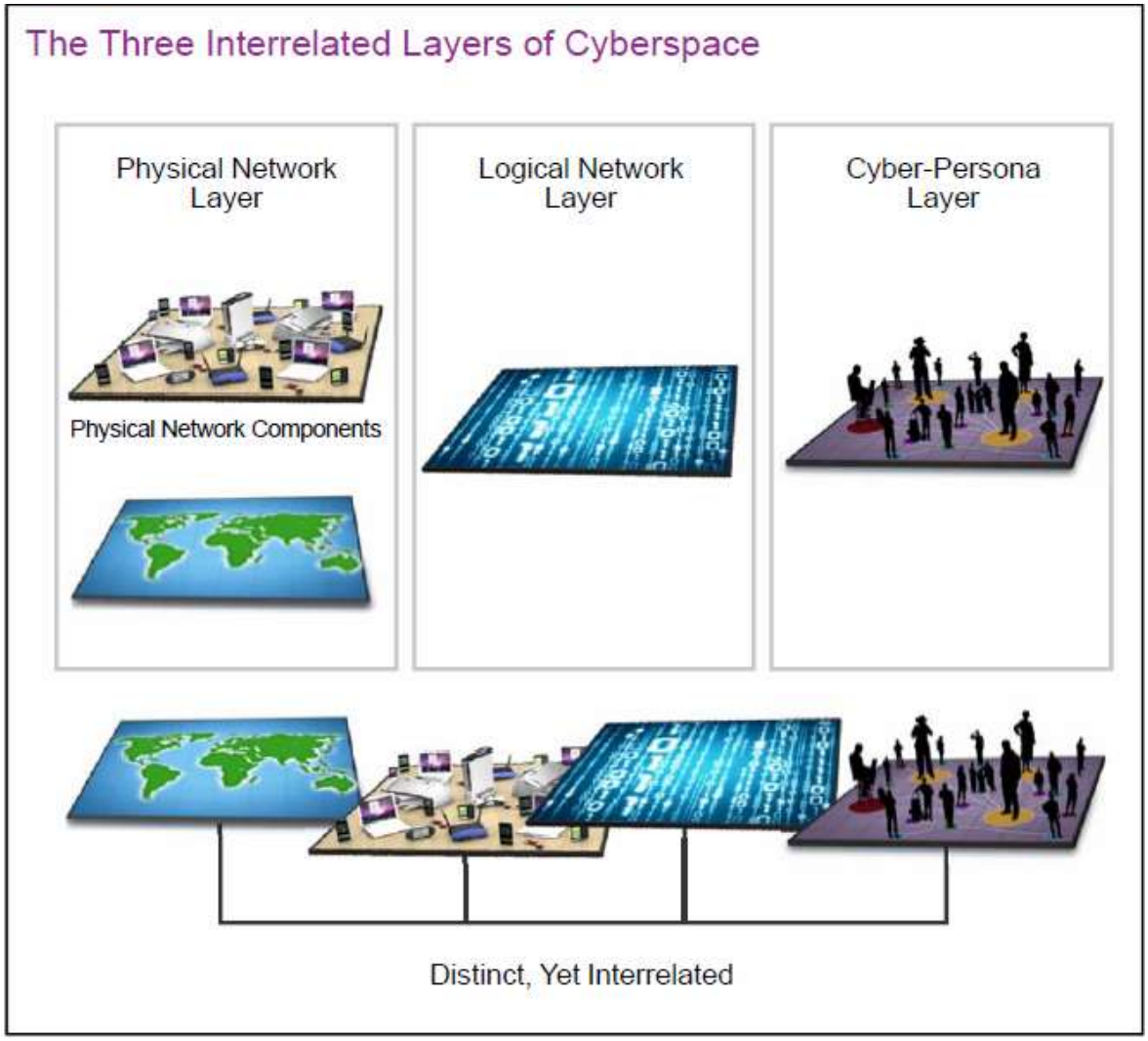

Figura 1 – As 3 camadas interligadas do ciberespaço

Fonte: JCS (2018).

Estas 3 camadas estão intimamente ligadas, de tal forma que a camada lógica não pode funcionar sem a camada física, e é a camada lógica que permite as *ciber-persona* atuem no ciberespaço (NATO, 2020). Cada uma das camadas pode ser alvo de uma operação no ciberespaço, mas alvos na camada lógica apenas podem ser alcançados com uma capacidade de natureza ciber (lógica) (Joint Chiefs of Staff , 2018).

Um dos princípios fundamentais da ENSC é o de que a segurança do ciberespaço é uma responsabilidade partilhada entre vários atores, sendo necessário uma abordagem holística que integre os diferentes os contributos, nomeadamente das FFAA, responsável pela ciberdefesa, e do CNCS, responsável pela cibersegurança (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019).

2.1.1.2 Cibersegurança

Há uma grande interdependência entre a ciberdefesa e cibersegurança, e muitas vezes, a fronteira que separa as mesmas é difusa, tanto a nível de recursos, quer humanos quer materiais (Nunes, 2018). Uma das atividades da ciberdefesa é a segurança dos CIS da Defesa Nacional, que é equivalente a dizer que é cibersegurança da Defesa (J.M. Vinagreiro, entrevista, 19 de abril de 2022). De um ponto de vista de coordenação e jurisdição, a ENSC identifica o CNSC como "[…] ponto de contacto único nacional para efeitos de cooperação internacional em matéria de cibersegurança, sem prejuízo das atribuições legais cometidas a outras entidades, nomeadamente, ao Ministério Público e à Polícia Judiciária, relativas a cooperação internacional em matéria penal, às Forças Armadas em matéria de ciberdefesa, ao Secretário-Geral do Sistema de Informações da República Portuguesa", indicando a necessidade de grande articulação nesta matéria (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2891). Num caso hipotético, havendo um ataque a uma infraestrutura crítica nacional, pode não haver certeza se o ataque é dirigido à organização dessa infraestrutura, aos seus clientes (cibersegurança), ou se tenciona causar prejuízo à nação (ciberdefesa), e quanto à fonte do ataque, se for um indivíduo ou grupo pequeno motivado por interesses próprios (cibercrime), ou uma ação perpetrada por uma nação adversária (ciberguerra) (Nunes, 2018). Internacionalmente foram reconhecidas três grandes áreas de atuação no ciberespaço, o combate ao cibercrime, a cibersegurança, e a ciberdefesa, que têm como alicerce, de forma transversal, os produtos dos serviços de informações (Jesus, 2021).

A definição de cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção tomadas no sentido de manter o estado de segurança desejado, garantindo a confidencialidade, integridade, disponibilidade e não repúdio da dos sistemas de informação e comunicação no ciberespaço, da informação e das pessoas que nele interagem (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019).

O CNSC tem como missão garantir que Portugal usa o ciberespaço de forma livre, confiável e segura, (Decreto-Lei n.º 136 de 6 de novembro, 2017). Para este desiderato, tem atribuídas várias competências, nomeadamente a execução do poder de autoridade nacional em matéria de cibersegurança, o desenvolvimento das capacidades nacionais de cibersegurança, contribuir para assegurar a segurança dos CIS do Estado e das infraestruturas críticas, promover a formação e qualificação de recursos humanos na área de cibersegurança,

coordenação e cooperação com entidades internacionais e nacionais em matérias de cibersegurança, ciberespionagem e ciberdefesa, entre outras (Decreto-Lei n.º 136 de 6 de novembro, 2017).

A Orientação para a Política de Ciberdefesa (Despacho n.º 13692, 2013), identifica a necessidade de haver parcerias entre instituições estatais e privadas, nacionais e internacionais, como forma de promover o desenvolvimento tecnológico, a investigação, formação, treino e a inovação, como é o caso do *Cyber Academia and Innovation Hub* (CAIH). Esta iniciativa, desencadeada pelo despacho do Ministério da Defesa Nacional (MDN) de 5 de março de 2021, tem como propósito constituir-se como um centro de excelência, interligando universidades, centros de investigação e a indústria das áreas de cibersegurança e ciberdefesa, segundo 3 vetores, formação treino e exercícios, investigação, desenvolvimento e inovação, e desenvolvimento da indústria ciber (Defesa Nacional, 2022b). O CAIH encontra-se situado tanto na área de cibersegurança como ciberdefesa, a nível nacional está alinhado com a ENSC, e a nível internacional com a política para a ciberdefesa da NATO, com as estratégias de cibersegurança da União Europeia (UE), e com países da Comunidade dos Países de Língua Portuguesa (Defesa Nacional, 2022b).

2.1.1.3 Desafios no uso do ciberespaço

O uso do ciberespaço apresenta vários desafios, alguns dos quais únicos a este domínio. As operações militares podem ser ameaçadas através do ciberespaço por nações, indivíduos, grupos de crime organizado, bem como por acidentes ou catástrofes naturais (JCS, 2018).

A facilidade de acesso ao ciberespaço, a disponibilidade de fontes de conhecimento técnico e ferramentas, permite a atores, que de uma forma convencional não conseguiriam, criar efeitos, globais, com pouco investimento, e de forma relativamente oculta e segura, tornando a avaliação da conjuntura global mais complicada, por não haver necessariamente uma ligação direta entre a *ciber-persona* e uma identidade no mundo real (EMGFA, 2022).

Neste contexto, importa estabelecer uma taxonomia de agentes que representam ameaças no ciberespaço:

- Atores estatais - possuem grandes recursos, podendo executar operações ofensivas ou de espionagem, quer de forma direta quer por recurso a terceiros, por forma a manter uma capacidade de negação plausível (EMGFA, 2022);
- Atores não estatais – estes atores, com objetivos próprios, podem usar o ciberespaço para conseguir os seus objetivos, ou podem ser contratados por

estados, quando o estado não possua as capacidades que precisa, ou quando o estado não queira ser associado às operações efetuadas, por questões políticas, legais ou éticas (NATO, 2020);

- Indivíduos ou pequenos grupos – atores que usam o ciberespaço, recorrendo a ferramentas de baixo custo, com motivações várias, como sejam recompensas financeiras, motivações políticas, entre outras (EMGFA, 2022);
- Acidentes e desastres naturais – a infraestrutura física do ciberespaço está exposta a acidentes humanos, acidentes industriais e desastres naturais, o que pode causar impacto nas operações de forma imprevisível. A recuperação destes eventos, pode sair fora da alçada das FFAA, por dependência de operadores privados ou estatais, representando uma dificuldade acrescida (EMGFA, 2022).

Além destes agentes referidos, as operações militares em destacamentos dependem de meios de comunicação que não são propriedade das FFAA que as executam, tendo que ser alugados a entidades internacionais ou privadas (JCS, 2018). Esta globalização das operações aumenta a dependência dos operadores dos serviços de comunicações, bem como de equipamentos comerciais necessários para o processamento, armazenamento e transmissão de dados, o que constitui uma vulnerabilidade no uso do ciberespaço (JCS, 2018).

O anonimato e a dificuldade de atribuição e responsabilização são uns dos grandes desafios do uso do ciberespaço, verificando-se grandes dificuldades em ligar uma *ciber-persona* a uma pessoa, grupo, organização ou nação de forma inegável (JCS, 2018).. A natureza do ciberespaço, bem como a moldura legal, nacional e internacional dificultam grandemente esta atribuição de responsabilidade por um determinado ato (JCS, 2018).

As questões legais, nomeadamente questões de jurisdição, de soberania, responsabilidade internacional e a lei dos ciber conflitos armados, representam mais uma das dimensões das dificuldades, ou desafios, do uso apropriado do ciberespaço, tendo sido criado o Manual de Tallinn, que representa um estudo em ciberguerra (lido como guerra através do ciberespaço) feito por um grupo internacional de especialistas legais (Schmitt, 2017).

O tribunal Internacional de Justiça determinou que a proibição do uso de força e da autodefesa aplicam-se a qualquer uso da força, independentemente da arma utilizada (Schmitt, 2017). O que está em causa não é o instrumento usado, um computador, por

exemplo, mas sim as consequências e o contexto desse uso (Schmitt, 2017). Em concreto, não são nem o alvo, nem o instrumento que estão em questão, mas sim se os efeitos de uma operação no ciberespaço ultrapassam o limiar do uso da força, por comparação a uma operação realizada num domínio que não o ciberespaço (Schmitt, 2017).

Em linha com este pensamento está o Secretário-Geral da NATO, Jens Stoltenberg, que afirmou em agosto de 2019 que "*A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all*" (Stoltenberg, NATO will defend itself, 2019), mas não foi explícito, sobre que tipo ou escala de ataque no ciberespaço provocaria a ativação do Artigo 5.º (Stoltenberg, Speech by Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, 2018). Esta afirmação foi deliberadamente vaga, para que não sejam públicas quais as "linhas vermelhas" da NATO, o que poderia permitir ataques abaixo desse limiar, sem receio de desencadear o Artigo 5.º (Prucková, 2022), conforme afirmado pelo Secretário-Geral da NATO "*The level of cyber-attack that would provoke a response must remain purposefully vague.*" (Stoltenberg, Speech by Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, 2018).

Em paralelo com a questão da determinação se um ciberataque pode ser considerado equivalente a um ataque armado, está também a questão da dificuldade de determinação da origem do ataque, já mencionada anteriormente, e no estabelecimento se essa origem é um Estado, para que se apliquem as regras do Direito dos Conflitos Armados/Direito Internacional Humanitário (Fernandes, 2014). Relevam para este efeito os atores não-estaduais, que podem ser instrumentalizados em guerras por procuração, como é o caso da China, que controla organizações não estatais que são proficientes em ciberguerra, ou da Rússia, que através da sua Rede de Negócios Russa funciona como plataforma facilitadora para ciberataques (Fernandes, 2014).

A concorrer com estas questões de legalidade, face aos efeitos provocados por uma operação no ciberespaço, a posse (Schmitt, 2017) e a localização da componente física, em termos geográficos, (NATO, 2020) são determinantes para estabelecer critérios de legalidade. Como tal, é importante distinguir o nosso ciberespaço, do ciberespaço adversário, do restante ciberespaço, surgindo as noções de Ciberespaço das Redes da Defesa Nacional (RDN), como todo o ciberespaço associado às CIS da Defesa Nacional, o Ciberespaço Azul, que indica áreas no ciberespaço das nações aliadas ou amigas que as FFAA, em conjunto com os seus parceiros de missão, podem vir a ser chamadas a proteger, Ciberespaço

Vermelho, às áreas do ciberespaço pertencentes ou controladas por nações potencialmente adversárias em contexto militar, e finalmente, o Ciberespaço Cinzento, que compreende todo o ciberespaço não englobado no Ciberespaço Azul ou Vermelho, considerando-se neutral (EMGFA, 2022).

2.1.2 Desenvolvimento da capacidade de ciberdefesa nacional

A Estratégia Nacional de Segurança do Ciberespaço (ENSC), de 2019, apontou como objetivos o reforço da capacidade de ciberdefesa nacional, atribuída às FFAA, de forma a "[…] fazer face a incidentes ou ciberataques significativos que afetem os interesses e a soberania nacionais" (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2891). Refere ainda a importância da "manutenção da capacidade de operação no ciberespaço através da capacidade de ciberdefesa defensiva." e assume que devem "[…] ser utilizados todos os meios para responder a ciberataques, incluindo a capacidade ofensiva no ciberespaço" (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2893).

A ENSC pretende também consolidar o "[…] Conselho Superior de Segurança do Ciberespaço como órgão específico de consulta do Primeiro-Ministro que assegure a coordenação político-estratégica para a segurança do ciberespaço, com representantes de todas as partes interessadas, que garanta uma abordagem transversal e inclusiva relativamente às políticas e iniciativas desenvolvidas pelas diversas entidades com responsabilidades neste âmbito", demonstrador da importância crescente desta matéria (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019, p. 2891).

Decorrente do CEDN e da ENSC, a LOEMGFA de 2022, que no seu sumário salienta "[…] o reforço da ação do Comando Conjunto para as Operações Militares (CCOM), nos domínios naval, terrestre, aéreo, espacial, cibernético e de informações, indispensável para a adaptação das Forças Armadas ao novo contexto global de segurança," (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022, p. 3), estabeleceu a criação do CCICE, já referido anteriormente, órgão de ciberdefesa que tem como missão assegurar "[…] o exercício do comando de operações militares no e através do ciberespaço" (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022, p. 22). Para este desiderato, tem o CCICE na sua dependência o Comando de Operações de Ciberdefesa (COCiber) com a responsabilidade de "[…] planear, dirigir, coordenar, controlar e executar operações no e através do ciberespaço em apoio a objetivos militares, garantindo a liberdade de ação das Forças Armadas neste domínio" (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022, p. 23).

O COCiber tem na sua estrutura o Estado Maior do COCiber, para o planeamento operacional, controle, condução e avaliação das operações no e através do, ciberespaço, e para a execução das várias operações no ciberespaço, conta com a Força de Operações de Ciberdefesa (FOCiber) (EMGFA, 2022). A FOCiber age segundo 3 linhas de operação, defender a RDN, contribuir para a defesa da nação de ataques no ciberespaço e prestar o apoio solicitado pelos Comandos Operacionais e Comandos de Força-Tarefa (EMGFA, 2022). O CEMGFA estabelece as Forças de Missão do Ciberespaço (FMCiber), equipas multidisciplinares específicas para cada missão, sob OPCON do COCiber, que são constituídas por unidades táticas (EMGFA, 2022):

- Equipa de Proteção do Ciberespaço (EPCiber) – realizam operações no ciberespaço (CISIO e DCO nos CIS da Defesa Nacional) para proteção interna dos CIS da Defesa Nacional;
- Equipa de Resposta no Ciberespaço (ERCiber) – realizam operações no ciberespaço (DCO em CIS não pertencentes à Defesa Nacional) para combater ameaças significativas aos CIS da Defesa Nacional;
- Equipa de Combate no Ciberespaço (ECCiber) – realizam operações no ciberespaço (OCO, CISRO) para apoiar as missões, planos e definição de prioridades dos Comandos Operacionais e Comandos de Força-Tarefa.

2.1.2.1 Operações no ciberespaço

As Operações no ciberespaço (OpsCiber) são operações militares, delimitados no tempo e espaço, onde se empregam capacidades de ciberdefesa, no ou através do ciberespaço, para atingir objetivos militares (EMGFA, 2022). A definição que consta no AJP 3.20 de operações no ciberespaço é de ações no ou através do ciberespaço, que pretendem manter a liberdade de ação no ciberespaço, e/ou criar efeitos para alcançar os objetivos do Comandante (NATO, 2020).

As OpsCiber podem ser Operações Defensivas no Ciberespaço (*Defensive Cyberspace Operations* - DCO), Operações Ofensivas no Ciberespaço (*Offensive Cyberspace Operations* - OCO), Operações na Infraestrutura de Comunicações e Sistemas de Informação (*Communication and Information Systems Infrastructure Operations* - CISIO) ou Operações de Informações, Vigilância e Reconhecimento no Ciberespaço (*Cyberspace Intelligence, Surveillance and Reconnaissance Operations* - CISRO), conforme figura 2 (EMGFA, 2022). Esta classificação não se prende com as ações efetuadas, com as forças atribuídas à missão,

nem com as capacidades de ciberdefesa utilizadas, mas sim com o objetivo do Comandante (EMGFA, 2022).

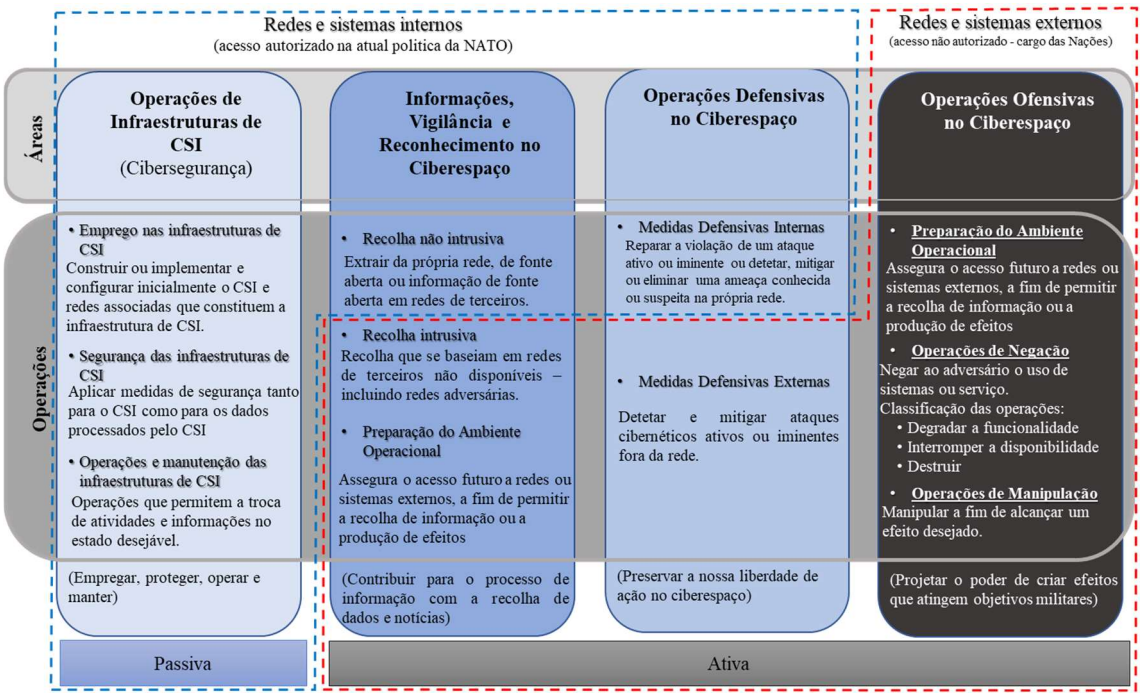

Figura 2 – Taxonomia de Operações no Ciberespaço

Fonte: EMGFA (2022).

Embora alguns objetivos possam ser conseguidos somente com operações no ciberespaço, essa não é a norma (JCS, 2018). Os Comandantes conduzem operações no ciberespaço para obterem ou manterem liberdade de manobra no ciberespaço, para atingirem objetivos do *Joint Force Commander* (JFC) e para permitirem outras atividades operacionais (JCS, 2018), e como tal, as operações no ciberespaço devem ser incluídas no processo de planeamento conjunto, de forma a facilitar a sincronização, unidade de esforço e coordenação do processo conjunto de escolha de alvos (NATO, 2020).

É importante relevar que, dado o cariz defensivo da NATO, a Aliança não procura ter, nem desenvolver capacidades ciber ofensivas, pelo que as OpsCiber desenvolvidas pela NATO terão sempre como linhas orientadoras prevenir, defender e recuperar de ciberataques, manter consciência situacional ciber, planear e manter C2 de OpsCiber (CCDCOE, 2022). Há, no entanto, um mecanismo, o *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA), que pode permitir que a NATO desencadeia OpsCiber ofensivas com efeitos que podem ser equivalentes a uso da força, mediante autorização do *North Atlantic Council* (CCDCOE, 2022). A integração de OpsCiber conduzidas ao abrigo do SCEPVA é treinada em exercícios, como o *Cyber Coalition* (CCDCOE, 2022).

2.1.2.1.1 Operações defensivas no ciberespaço

As operações defensivas no ciberespaço consistem nas medidas para a manutenção da capacidade de utilização do ciberespaço garantindo a liberdade de ação e para proteção da força (NATO, 2020). As DCO podem ser Medidas Defensivas Internas (*Internal Defensive Measures* IDM), que são ações de defesa que ocorrem dentro da rede defendida, e feitas de forma permanente, ou Ações de Resposta (*Response Actions* RA), em que as ações são realizadas fora da rede defendida, sem autorização do proprietário do sistema afetado, necessitando para tal de uma ordem militar devidamente coordenada (EMGFA, 2022).

O JP 3.12 define as operações defensivas no ciberespaço como missões para defender o ciberespaço pretendido de ameaças neste ciberespaço, quer sejam iminentes, quer estejam já a decorrer (JCS, 2018).

2.1.2.1.2 Operações ofensivas no ciberespaço

As OCO tencionam projetar poder no e através do ciberespaço. Baseiam-se na manipulação ou disrupção de redes e sistemas com o propósito de limitar ou eliminar a capacidade operacional do adversário (EUMS, 2016). As OCO podem ter como alvo funções no ciberespaço adversário, ou podem criar efeitos que afetem sistemas de armas, sistemas de C2, sistemas logísticos ou alvos de elevado valor, etc. (JCS, 2018).

2.1.2.1.3 Operações na Infraestrutura de Comunicações e Sistemas de Informação

As ações e medidas referidas na definição de cibersegurança, efetuam-se no ciberespaço, para impedir acessos não autorizados, exploração ou danos nos sistemas de informação e comunicação, na informação neles contida, protegendo-os de ameaças no ciberespaço, reduzindo ou eliminando as vulnerabilidades, que podem ser exploradas por adversários (EMGFA, 2022).

As operações CISIO têm como objetivo assegurar a cibersegurança da RDN, incluindo redes táticas utilizadas por forças projetadas, sendo realizadas pelas Componentes de Segurança dos CIS do EMGFA, Ramos ou do Centro de Dados da Defesa, sob auditorias do Comando de Operações de Ciberdefesa (COCiber) e constituem-se como uma missão permanente (EMGFA, 2022).

2.1.2.1.4 Operações de Informações, Vigilância e Reconhecimento no Ciberespaço

As CISRO têm como objetivo a recolha de informação, vigilância e reconhecimento, conduzidas no ciberespaço, contribuindo para a produção de informações, podendo assumir

a forma de operações não intrusivas, que recorrem a fontes abertas, operações intrusivas, visando fontes não publicamente disponíveis, incluindo os CIS adversários, e operações de preparação do ambiente operacional, que de forma intrusiva garantem acesso futuro a redes ou sistemas externos, para recolha de informação (EMGFA, 2022).

2.1.2.2 Formação e Treino

Explanada a orgânica da Ciberdefesa Nacional, para que seja possível a execução das OpsCiber, são necessários recursos humanos devidamente formados e treinados (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022). Para garantir esta formação e a sustentação continuada destes elementos, a LOEMGFA prevê na constituição do CCICE a Escola de Ciberdefesa (ECD) (Lei Orgânica n.º 2/2019 de 17 de junho, 2019). O COCiber, para o cumprimento da sua missão, tem ao seu dispor elementos recrutados e treinados pelos ramos, com o apoio da ECD, e através de um processo de alinhamento da missão para a geração de forças de ciberdefesa, conforme os requisitos de cada missão, constitui equipas multidisciplinares específicas, as já mencionadas FMCiber (EMGFA, 2022).

Além da formação dos elementos pertencentes à ciberdefesa, deve ser focada a questão do treino, por via de participação em exercícios nacionais e internacionais, em contexto de cibersegurança e ciberdefesa, que se assume como uma mais-valia, para todos os níveis envolvidos (Jesus, 2021). Em termos de exercícios internacionais, a NATO assiste os aliados no desenvolvimento de capacidades de ciberdefesa através da partilha de boas práticas e de informação, nomeadamente através da NATO *Malware Information Sharing Platform* e pela condução de exercícios que permitem às nações incrementar os conhecimentos e experiências nesta área (NATO, 2022a). O *Cyber Coalition* é o exercício NATO mais importante em matéria de ciberdefesa, planeado e conduzido anualmente pelo *Allied Command Transformation*, sob o comando do *Military Committee*, com a finalidade de reforçar as capacidades da Aliança para parar, defender e contrariar ameaças no e através do ciberespaço, em suporte das atividades fundamentais da NATO, permitindo o treino coordenado de operações no ciberespaço, e feedback para a transformação e evolução da NATO (NATO, 2022b). O *Cyber Coalition* é executado através da *Estonian Cyber Security Exercises and Training Centre*, localizada em Tallinn, também designada como CR14, uma *cyber range*[1] da NATO, que permite que a audiência de treino participe a partir das suas nações, através de redes virtuais (NATO, 2022b). Além deste exercício de renome, os

[1] Cyber range – ambiente virtual, interativo, que simulam um ou vários CIS, para efetios de treino e aumento de proficiência no uso de competências ciber (NIST, 2022)

exercícios *Locked Shields* (CCDCOE, 2022a) e *Crossed Swords* (CCDCOE, 2022b), apoiados pelo *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), são também exercícios de ciberdefesa, o primeiro, equipa azul, para treinar a proteção de CIS, militares e civis, o segundo, equipa vermelha, para treinar a ofensiva (CCDCOE, 2022b).

2.1.2.3 NATO CD-DEPLOY

Como forma de providenciar uma linguagem comum para a definição de capacidades no planeamento de defesa e no planeamento operacional, foi aprovado o *Capability Codes and Capability Statements* (CC&CS) pelo *Bilateral Strategic Command* (NATO, 2016a). Este documento foi empregue pela primeira vez em 2004, tendo sido sujeito a revisões e melhorias em linha com os ciclos de planeamento da NATO, o NDPP, e está organizado em áreas e subáreas, dentro das quais estão os vários CC (NATO, 2016a). Cada *Capability Code* (CC) possui uma estrutura, que permite perceber os elementos essenciais e os efeitos que o CC pretende atingir (NATO, 2016a):

- *Capstone Capability Statement* - explicam o propósito fundamental do CC;
- *Principal Capability Statements* - o que o CC tem que fazer de forma a atingir os efeitos desejados, com enfoque em capacidades operacionais;
- *Enabling Capability Statements* - Descreve as características que o CC precisa para conseguir concretizar as atividades operacionais descritas pelas *Capstone Capability* e pelos *Principal Capability Statements*.

O CC&CS de 2016 define, dentro da área de Defesa, subárea Ameaças Ciber, 2 CC, o CD-DEPLOY com a designação de ciberdefesa projetável, "*Deployable Cyber Defence*",, foco deste trabalho, e o CD-STATIC com designação ciberdefesa estática de *Static Cyber Defence*[2], com um descritor e 19 *Principal Capability Statements* que são comuns a ambos os CC, ciberdefesa estática e ciberdefesa projetável, e cujo conteúdo se encontra no anexo A (NATO, 2016a).

O *Capstone Capability Statement* do CD-DEPLOY identifica como propósito principal a capacidade de aplicar medidas de segurança em redes destacadas para proteger os sistemas de informação e comunicação, e outros sistemas eletrónicos, e a informação que por eles é armazenada, protegida ou transmitida, no tocante à confidencialidade, integridade, disponibilidade, autenticação e não-repúdio (NATO, 2016a). Os *Principal Capability Statements* listados, estão associados às capacidades da figura 3, e de forma sucinta, descrevem atividades de proteção ou mitigação contra ataques aos CIS e à informação por

[2] Ciberdefesa estática – entendido como capacidade de ciberdefesa para CIS não projetáveis

eles armazenada, processada e transmitida, controlo de acessos, encriptação, controlo de configurações, monitorização, gestão de risco, continuidade de serviço, análise de informação de segurança do CIS, e reporte de informação de segurança (NATO, 2016a). Os *Principal Capability Statements* 2.20 e 2.21 (ver anexo A), específicos do CD-DEPLOY, referem-se à capacidade de projetar um módulo escalável [3]e modular[4] que possa ser adaptado a todo o tipo de CIS projetáveis em termos de tamanho, complexidade e distribuição geográfica (NATO, 2016a).

Nos *Enabling Capability Statements* constam a capacidade de ser projetado num teatro para operações em todo o espetro das missões da NATO, incluindo combate de alta intensidade, capacidade para ser integrado numa unidade projetada de CIS, capacidade de projetar uma equipa para suporte de unidades subordinadas do Comando apoiado, em caso de incidente ciber, capacidade de ser integrado numa unidade de escalão superior ou instalação que lhe forneça apoio logístico e proteção, e capacidade de apoiar a proteção de uma infraestrutura crítica civil (NATO, 2016a).

Para esclarecer requisitos técnicos relativos ao CD-DEPLOY, foi desenvolvido pela NATO *Communication and Information Agency* (NCIA), o *Deployable Cyber Defence Reference Capability version 1.1*, um relatório técnico que pode ser utilizado como *benchmark* para o desenvolvimento desta capacidade, e que teve como elemento fundamental o suporte em termos de ciberdefesa a *Deployable Communication and Information Systems* (DCIS), e como tal foi enquadrado por documentação relativa à segurança de CIS, cujos pilares podem ser vistos na figura 3 (NATO Communications and Information Agency, 2016).

[3] Escalável – que pode crescer sem impacto para a missão
[4] Modular – agrupado ou dividido de forma funcional

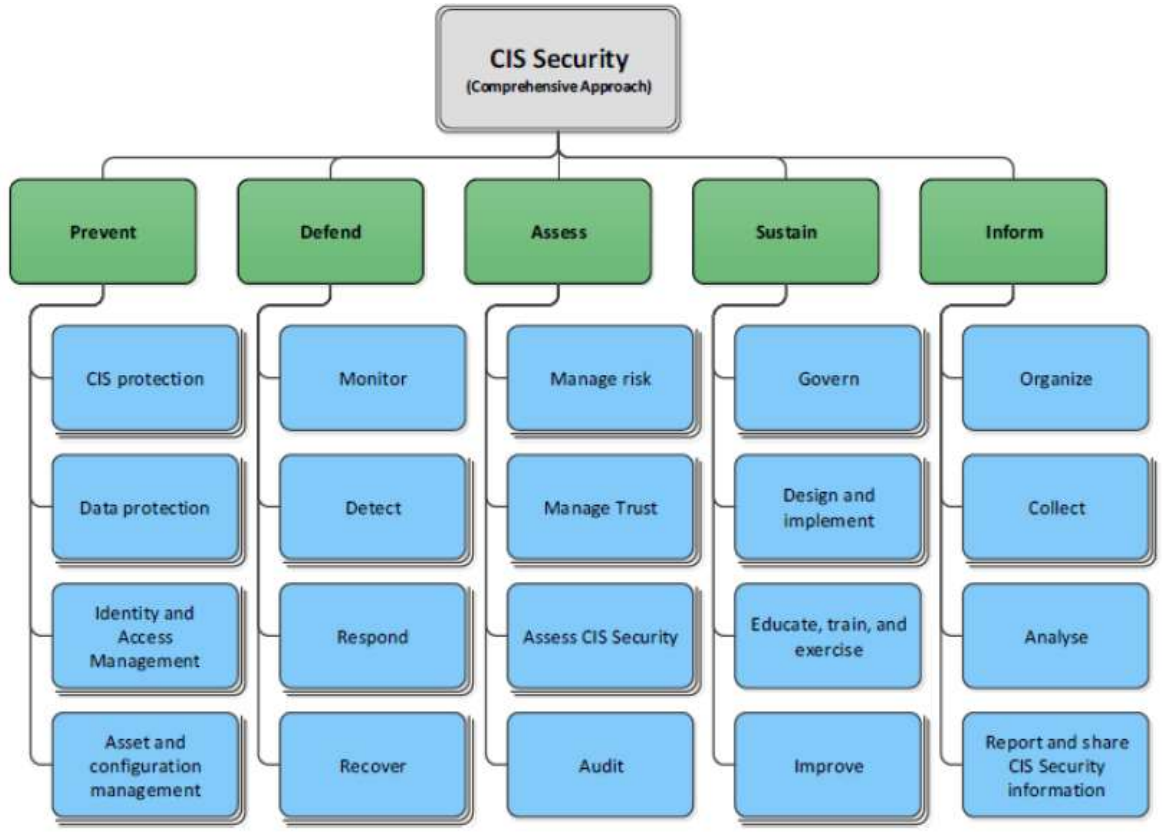

Figura 3 – Estrutura das capacidades do CIS *Security*

Fonte: NCIA (2016).

Os requisitos para CD-DEPLOY, podem ser estruturados como procedimentos (P[5]), competências especializadas (S[6]), ferramentas (*software* ou mecanismo) (T[7]) e ativos (*hardware* ou infraestrutura) (A[8]), que podem ser cruzados com a informação constante no anexo A permitindo identificar ativos específicos como *firewalls*, *software* para análise de *emails*, pessoal treinado para análise de incidentes e procedimentos que permitam a partilha de informação respeitante a incidentes de cibersegurança, entre outros (NATO Communications and Information Agency, 2016).

O *Deployable Cyber Defence Reference Capability version 1.1* esclarece que as atividades de ciberdefesa previstas no CD-DEPLOY limitam-se essencialmente às atividades de cibersegurança, excluindo desta capacidade todas as operações no ciberespaço efetuadas fora na nossa infraestrutura (NATO Communications and Information Agency, 2016).

[5] Procedures
[6] Specialised Skill Sets
[7] Specialised Tools
[8] Assets

2.2 Modelo de análise

No Apêndice A consta o modelo de análise que orientou esta investigação.

3. Metodologia e método

Neste capítulo são descritos a metodologia e o método que direcionaram o rumo deste trabalho de investigação, que pretende contribuir para a certificação das FFAA Portuguesas na capacidade NATO CD-DEPLOY, para que melhor possamos desempenhar o nosso papel no compromisso que temos com a Aliança NATO.

3.1 Metodologia

A metodologia que foi seguida na elaboração deste trabalho assenta numa investigação de raciocínio indutivo, utilizando uma estratégia mista, baseada em análise documental e entrevistas semiestruturadas (Santos & Lima, 2019).

3.2 Método

O método usado para recolher informação foi análise de documentação proveniente da NATO, UE, Forças Armadas dos EUA, e das FFAA nacionais sobre ciberdefesa. Também foram feitas entrevistas semiestruturadas, conforme descrito de seguida no procedimento.

3.2.1 Participantes e procedimento

As entrevistas semiestruturadas foram entregues ao órgão de planeamento e execução na ciberdefesa nacional. Foram feitas várias entrevistas, complementares, com teor ajustado ao progresso do trabalho.

3.2.2 Instrumentos de recolha de dados

No que diz respeito à recolha de dados, foram utilizados dois instrumentos distintos, a análise documental e entrevistas semiestruturadas.

Foi feita uma entrevista para o responsável pelo COCiber, uma vez que é o Órgão com responsabilidade pelo planeamento, direção, coordenação, controlo e execução de operações no e através do ciberespaço. Na sequência do trabalho, foram feitas outras 3 entrevistas ao COCiber, para obter informação mais concreta em termos das capacidades das FFAA em matéria de ciberdefesa.

4. Apresentação dos dados e discussão dos resultados

Neste capítulo é analisada a informação recolhida da análise documental e das entrevistas, para responder às Questões Derivadas e à Questão Central.

4.1 Requisitos da capacidade NATO CD-DEPLOY

Da análise do CC CD-DEPLOY, e tendo em conta que dos 21 *Principal Capability Statements*, 19 são comuns ao CC CD-STATIC, e tendo em conta o teor dos mesmos, já abordado anteriormente, pode-se retirar que o foco do CD-DEPLOY é a proteção em termos de ciberdefesa de um CIS projetável (NATO Communications and Information Agency, 2016). É importante referir que esta proteção em termos de ciberdefesa consiste essencialmente em operações CISIO, que conforme mencionado anteriormente, é uma componente das operações passiva (EMGFA, 2022), em tudo semelhante à atividade de cibersegurança, como se pode ver da sobreposição da definição de cibersegurança (Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho, 2019) e o *Capstone Capability Statement* do CD-DEPLOY (NATO, 2016a).

Da análise do relatório técnico, retirou-se um conjunto de requisitos, que ambos os CC CD-DEPLOY e CD-STATIC terão que implementar, que foram cruzados com os requisitos mínimos de segurança de um CIS, dando origem aos requisitos mínimos e desejáveis (ver anexo B) (NATO Communications and Information Agency, 2016).

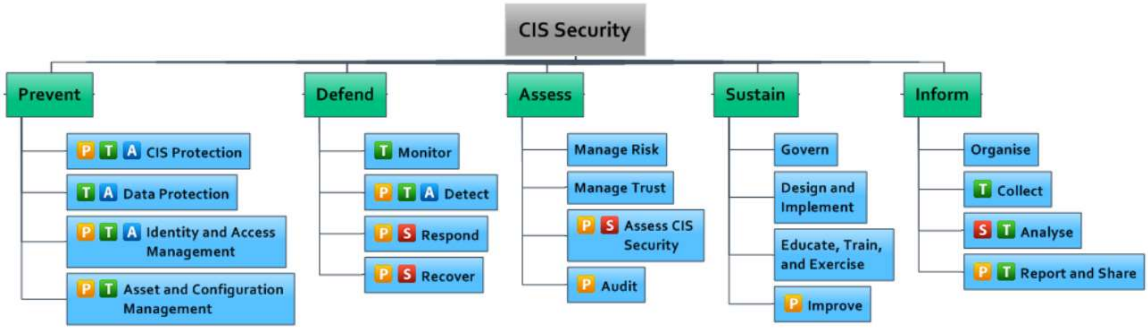

Figura 4 – Requisitos mínimos de segurança de CIS

Fonte: NCIA (2016).

Todos os blocos azuis, que representam atividades de CIS, que contenham um recurso P, T, S ou A, estão explicitamente abrangidos pelo CD-DEPLOY, pelo que são de implementação obrigatória, logo requisitos mínimos (NATO Communications and Information Agency, 2016). As atividades de CIS que não contenham recursos P, T, S ou A, não constituem requisitos mínimos para o CC CD-DEPLOY, mas sim requisitos desejáveis (NATO Communications and Information Agency, 2016).

Estes requisitos foram agrupados, sobre um prisma mais técnico, com indicação dos recursos necessários, e podem ser visualizados na tabela 1:

Tabela 1 – Requisitos mínimos do CC CD-DEPLOY

Requisitos do CD-DEPLOY	Tipo Recurso
Equipa de resposta a incidentes	P S T A
Analistas de ciberdefesa	P S T A
Gateway e/ou *Data Diode*	A
Firewall, *anti-virus* e *anti-malware*	T A
Sistemas de deteção/prevenção de intrusão em redes e *hosts*	P T S A
Equipamentos criptográficos e sistemas de gestão de chaves criptográficas	P T A
Sistema de *data labelling and binding*	P T A
Sistema *Public Key Infrastructure* (PKI)	P S T A
Sistema de gestão de credenciais	P S T A
Gestão de informação documental classificada	P A T
Online Computer Forensic	P T
Online Vulnerability Assessment	P T
Security Information and Event Management	P T
Full Packet Capture	
Sistema de reporte de segurança CIS automático	P T
CIS *Security Situation Awareness Decision Support*	P S T
Sistema de gestão de configurações	P T A
Sistema de gestão de risco	P T
Sistema de gestão de incidentes e procedimentos de recuperação	P S T
Sistema de *backup*	P S T
Processo de lições aprendidas	P

Fonte: Adaptado de NCIA (2016).

Legenda:

P - *Procedures*

S - *Specialised Skill Sets*

T - *Specialised Tools*

A – *Assets*

Da análise da tabela 1, e conforme mencionado anteriormente, podemos ver que os requisitos estão agrupados em procedimentos, competências especializadas, ferramentas (software ou mecanismo) e ativos (hardware ou infraestrutura), podendo ser agrupados em recursos humanos, técnicos com formação e competências específicas, nos domínios de análise forense e resposta a incidentes, entre outras, recursos materiais, tais como Sistemas de deteção/prevenção de intrusão em redes e *hosts* ou *Data Diode*, e procedimentos que

indicam como deve ser uma atividade executada (NATO Communications and Information Agency, 2016).

4.2 Capacidades da FFAA Portuguesas em matéria de ciberdefesa

A nível das FFFAA Portuguesas, e conforme explanado anteriormente, a LOEMGFA estabeleceu a criação do CCICE como órgão de ciberdefesa nacional, exercendo o comando de operações militares no e através do ciberespaço (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022). O CCICE, no âmbito das FFAA, órgãos e serviços do MDN, tem autoridade técnica, sobre a segurança e os sistemas de informação, e autoridade técnica e funcional no âmbito da ciberdefesa, tendo como atribuições para este desiderato, além da já mencionada ciberdefesa, o planeamento, sustentação e execução das medidas de segurança e resposta a incidentes dos CIS, bem como o desenvolvimento das capacidades nacionais destinadas a fazer face a incidentes de cibersegurança e ciberataques (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022).

Na dependência do CCICE, está o COCiber, responsável pelo planeamento, controlo e execução de operações no e através do ciberespaço, recorrendo às FOCiber, que através das FMCiber, com recurso a várias equipas multidisciplinares, realizam a nível tático as várias operações no ciberespaço (EMGFA, 2022). No âmbito puro de ciberdefesa, entendida como operações no ciberespaço cujo objetivo não sejam a cibersegurança, a estrutura do COCiber pode ser reforçada por elementos ou unidades dos ramos, designadamente em estado de guerra e em estados de exceção, bem como o planeamento e condução de exercícios conjuntos ou combinados (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022).

Em termos de cibersegurança nas FFAA, os ramos são responsáveis pela resposta a incidentes dos seus CIS, defendendo o seu segmento do Ciberespaço Azul, sob coordenação do COCiber (EMGFA, 2022). Havendo um incidente que o ramo não consiga resolver de forma autónoma, o COCiber assume o controlo tático (TACON) do órgão de ciberdefesa do ramo, ficando responsável pela resposta ao incidente (EMGFA, 2022). Esta estrutura é ilustrada pela figura 5.

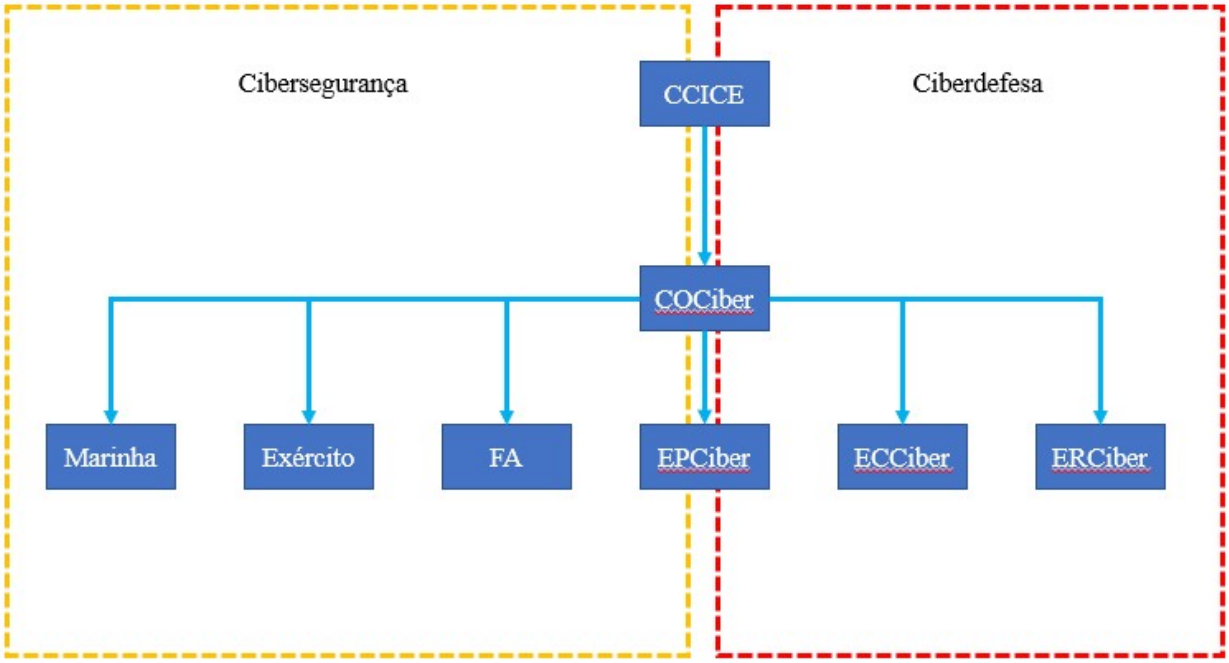

Figura 5 – Ciberdefesa incluída e excluída no NATO CD-DEPLOY

Fonte: Adaptado de EMGFA(2022)

O relatório técnico identifica nos requisitos do CC CD-DEPLOY, recursos humanos com competências especializadas (NATO Communications and Information Agency, 2016). Quanto a este fator, a ECD está presentemente a formar 22 elementos, prevendo-se a admissão anual de 25 militares para ciberdefesa, como forma de sustentar a componente humana desta capacidade, não se prevendo desta forma constrangimentos desta natureza para a implementação da capacidade CD-DEPLOY (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022).

Com a intenção de verificar se as FFAA cumprem com os requisitos mínimos para implementação do CC CD-DEPLOY, foi feita uma entrevista ao TC Jorge Vinagreiro, Chefe do COCiber, sendo o resultado apresentado na tabela 2.

Tabela 2 – Cumprimentos dos requisitos mínimos pelas FFAA Portuguesas

Requisitos do CD-DEPLOY	Tipo	Capacidade nacional
Equipa de resposta a incidentes	P S T A	Sim
Analistas de ciberdefesa	P S T A	Sim
Gateway e/ou *Data Diode*	A	**Sim***
Firewall, *anti-virus* e *anti-malware*	T A	Sim
Sistemas de deteção/prevenção de intrusão em redes e *hosts*	P T S A	Sim
Equipamentos criptográficos e sistemas de gestão de chaves criptográficas	P T A	Sim
Sistema de *data labelling and binding*	P T A	**Sim***

Sistema *Public Key Infrastructure* (PKI)	P S T A	Sim
Sistema de gestão de credenciais	P S T A	Sim
Gestão de informação documental classificada	P A T	Sim
Online Computer Forensic	P T	**Sim***
Online Vulnerability Assessment	P T	**Sim***
Security Information and Event Management	P T	Sim
Full Packet Capture		Sim
Sistema de reporte de segurança CIS automático	P T	Sim
CIS *Security Situation Awareness Decision Support*	P S T	**Não**
Sistema de gestão de configurações	P T A	Sim
Sistema de gestão de risco	P T	**Não**
Sistema de gestão de incidentes e procedimentos de recuperação	P S T	Sim
Sistema de *backup*	P S T	Sim
Processo de lições aprendidas	P	**Sim***

Fonte: Adaptado de NCIA (2016).

Legenda:

P – *Procedures*

S – *Specialised Skill Sets*

T – *Specialised Tools*

A – *Assets*

Sim* – requisitos parcialmente concluídos

Da análise da tabela 2, pode-se retirar que não se consegue cumprir os requisitos CIS *Security Situation Awareness Decision Support* e Sistema de gestão de risco. Em relação ao CIS *Security Situation Awareness Decision Support*, a capacidade CD-DEPLOY terá que contar com uma plataforma *Cyber Situational Awareness*, mas este conceito encontra-se ainda em desenvolvimento, pelo que o nível de maturidade ainda não é suficiente para esta implementação (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022). Quanto ao Sistema de gestão de risco, o CCICE tem este tipo de plataformas ao seu dispor, mas há necessidade de ajuste dos processos relativos à gestão de risco, para a capacidade CD-DEPLOY (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022).

Em relação aos requisitos *Online Computer Forensic* e *Online Vulnerability Assessment*, o COCiber possui plataformas para este efeito, faltando apenas pessoal treinado para este fim, mas esse processo já está em desenvolvimento (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022). O requisito de possuir um Sistema de *data labelling and binding* não está na dependência do COCiber, mas do CCICE, e está também em processo de desenvolvimento, assim como as soluções *Gateway* e/ou *Data Diode*, que também estão na dependência do CCICE, e terão que ser planeados conforme os requisitos operacionais e

alinhados com a *Federated Mission Network* (FMN), não se antecipando constrangimentos (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022). Quanto ao requisito de lições aprendidas relativas ao CD-DEPLOY, este terá que ser integrado no processo de Lições Aprendidas no Centro de Avaliação, Certificação e Lições Aprendidas (CACLA), inserido no CCOM, EMGFA (J.M. Vinagreiro, entrevista por *email*, 20 de junho de 2022).

4.3 Medidas a implementar para alcançar a certificação das FFAA NATO CD-DEPLOY

Analisadas as capacidades das FFAA em matéria de ciberdefesa, e os requisitos para a implementação do CC CD-DEPLOY, é possível inferir que em termos orgânicos as FFAA Portuguesas têm uma orgânica que coloca o CCICE, órgão de comando da ciberdefesa, na dependência direta do CEMGFA, com o COCiber, órgão de planeamento, controlo e execução de ciberdefesa (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022). O COCiber,para execução das operações no ciberespaço, constitui em função dos requisitos da missão, equipas multidisciplinares de nível tático, FMCiber, para a execução de operações no ciberespaço (EMGFA, 2022). Em termos de ciberdefesa na vertente de cibersegurança, operações CISIO e DCO IDM, o COCiber conta com a EPCiber e com a componente de ciberdefesa dos Ramos das FFAA (EMGFA, 2022).

Deste ponto de vista orgânico, não foram identificadas medidas relevantes para assistir na implementação da capacidade NATO CD-DEPLOY.

Em termos de formação e qualificação de recursos humanos para a área de ciberdefesa, a ECD tem capacidade para formação de forma sustentada de técnicos, pelo que não foram identificadas neste prisma medidas relevantes para a implementação do NATO CD-DEPLOY.

O EMGFA considera essencial a participação em exercícios nacionais e internacionais, como forma de capacitar os elementos que constituem a ciberdefesa, estando esta participação prevista doutrinariamente, embora não tenha havido a participação com o nível desejável, desde 2020, por motivos relacionados com a pandemia COVID-19 (J.M. Vinagreiro, entrevista por *email*, 7 de julho de 2022). Foi aqui identificada uma medida para implementação (MI), MI1, que se prende com a retoma da participação regular em exercícios nacionais e internacionais, de cariz ou com uma componente ciber, seja cibersegurança ou ciberdefesa, como forma de consolidar conhecimentos, aumentar a proficiência técnica e desenvolver a interoperabilidade com as nações Aliadas.

Da análise da tabela 2, em relação aos requisitos *Online Computer Forensic* e *Online Vulnerability Assessment*, falta capacitar elementos do COCiber para a operação destas plataformas, tendo sido esta situação identificada como a MI2.

Foi identificada a MI3 relacionada com o processo de aquisição do Sistema de *data labelling and binding*, pelo CCICE.

Foram identificadas a MI4 que se prende com o ajuste dos processos para o Sistema de gestão de risco e a MI5, que esta relacionada com a integração do processo de lições aprendidas no CACLA.

5. Conclusões

A NATO, organização de defesa coletiva, inclui a ciberdefesa como parte integrante das suas funções desde 2014, tendo reiterado a importância crescente desta componente diversas vezes, culminando no reconhecimento do ciberespaço como um domínio operacional. Esta importância que a NATO tem demonstrado relativamente às capacidades ciber, ficou patente ao reconhecer que um ciberataque a um país Aliado pode desencadear a ativação do Artigo 5º, ao mesmo tempo que, de forma deliberada e não explícita, não define que tipo de ciberataque, ou que consequências teria que ter, para despoletar a defesa coletiva das restantes nações Aliadas. Esta orientação à questão ciber, tem levado a NATO a desenvolver internamente uma cultura de cibersegurança e a incentivar o desenvolvimento de capacidades de ciberdefesa, junto das nações Aliadas. Nesta linha de atuação, como forma de fomentar o desenvolvimento nacional dos parceiros NATO, a capacidade de ciberdefesa passou a integrar o *NATO Defence Planning Process,* tendo sido criada uma subárea Ameaças Ciber, que inclui requisitos de segurança dos CIS, tanto estáticos, como projetados. Em 2016 foi criado o NATO CD-DEPLOY, um CC específico para CIS projetáveis, fulcral para o tema deste estudo.

Portugal, como nação aliada, tem desenvolvido esforços para aumentar a resiliência do seu ciberespaço, em termos de cibersegurança, através do CNCS, e em termos de ciberdefesa, através das FFAA, em concreto do CCICE/COCiber, estando inscrito em LPM valores crescentes para os programas de ciberdefesa. Vários documentos demonstram a importância desta temática, desde a Diretiva Estratégica do EMGFA 2018/2021, passando pela ENSC, e a mais recente LOEMGFA, de janeiro de 2022, com alterações orgânicas na área da ciberdefesa.

Este trabalho centrou-se na capacidade de ciberdefesa destacável NATO CD-DEPLOY, procurando desenvolver medidas que permitam a certificação das FFAA nessa capacidade.

Este estudo foi delimitado espacialmente aos órgãos e entidades das FFAA com responsabilidade especifica na ciberdefesa nacional, temporalmente ao período de novembro de 2010 a julho de 2022, e em termos de conteúdo, refere-se apenas às capacidades de ciberdefesa das FFAA.

Este trabalho iniciou-se com o estudo da doutrina Nacional, NATO, UE, JCS, entre outras, centrado no tema da ciberdefesa, começando pelo domínio no qual a ciberdefesa assenta, o ciberespaço, abordando todos os desafios que o seu uso e exploração trazem,

destacando a anonimização e consequente dificuldade de responsabilização de atos efetuados no ou através do ciberespaço, questões de legalidade e jurisdição, nacional e internacional, e inclusive de soberania, e pela dependência dos órgãos estatais de operadores de serviços de comunicação, com a respetiva diminuição da autonomia. Neste contexto de desafios associados ao uso do ciberespaço, foram também abordados quais os tipos de agentes que representam diferentes ameaças. Foi abordado o tema da cibersegurança, por estar intimamente relacionado com a ciberdefesa do ciberespaço, tendo que haver grande articulação entre estas componentes da proteção do ciberespaço, a cibersegurança e a ciberdefesa, bem como com órgãos de investigação criminal e serviços de informação. Quanto ao tema da ciberdefesa, foram estudados os vários tipos de operações no ciberespaço, as operações defensivas do ciberespaço, que pretendem manter a capacidade de utilização do ciberespaço e proteção da força, realizadas tanto em ciberespaço azul como fora deste, as operações ofensivas no ciberespaço, que tencionam projetar poder no e através do ciberespaço para reduzir ou eliminar a capacidade operacional adversária, as operações na infraestrutura de comunicações e sistemas de informação, protegendo os CIS e a informação que neles consta, e as operações de informações, vigilância e reconhecimento no ciberespaço, que têm como objetivo a recolha de informação, vigilância e reconhecimento contribuindo para a produção de informações, que podem ser efetuadas de forma não intrusiva ou intrusiva, conforme sejam efetuadas em ciberespaço azul, ou fora deste, respetivamente. Foi também explicado o mecanismo SCEPVA, que permite que a NATO integre capacidades ofensivas de natureza ciber provenientes de Aliados, uma vez que a NATO como organização defensiva não possui, nem pretende possuir ou desenvolver capacidades ciber ofensivas. Foram distinguidas as operações que são realizadas no ciberespaço da nossa responsabilidade, das operações que são realizadas no ciberespaço de terceiros, e foi também explanada a integração das operações no ciberespaço com outras operações. Após compreensão deste conceito estruturante, foram analisados o CC&CS 2016 e o relatório técnico *Deployable Cyber Defence Reference Capability version 1.1*, para compreender as implicações e os requisitos da capacidade NATO CD-DEPLOY, que foi estruturado tendo como base a segurança de CIS e de DCIS, tendo-se concluído que esta capacidade assenta essencialmente na cibersegurança do CIS projetado, excluindo-se desta capacidade todas as operações fora do ciberespaço do CIS das forças projetadas. Desta forma, as operações no ciberespaço que a capacidade NATO CD-DEPLOY compreende são Operações na Infraestrutura de Comunicações e Sistemas de Informação, Operações de

Informações, Vigilância e Reconhecimento no Ciberespaço – não intrusivas, e Operações Defensivas no Ciberespaço – Medidas de Defesa Interna. Um produto essencial desta análise para a consecução deste trabalho foi a produção de uma listagem de requisitos mínimos para a implementação da capacidade NATO CD-DEPLOY, agrupados em procedimentos, elementos com competências especializadas, ferramentas e ativos, que permite responder à QD1, "*Quais os requisitos para a capacidade de ciberdefesa destacável NATO CD-DEPLOY?*", atingindo desta forma o OE1, "*Analisar a capacidade de ciberdefesa destacável NATO CD-DEPLOY.*".

Para cumprir com o OE2, "*Analisar as capacidades das FFAA Portuguesas em matéria de ciberdefesa*", procurando desta forma responder à QD2, "*Quais as capacidades das FFAA Portuguesas em matéria de ciberdefesa?*" foi estudada a orgânica nacional da ciberdefesa, com destaque para o CCICE, órgão de ciberdefesa na dependência direta do CEMGFA, com a missão de comando de operações militares no ciberespaço, e o COCiber, na dependência do CCICE, que planeia, controla e executa as operações no ciberespaço, recentemente estabelecidos pela LOEMGFA. O COCiber tem controlo operacional sobre as FMCiber, que têm várias equipas, EPCiber, ERCiber e ECCiber, que executam as missões ao nível tático. Para a segurança do ciberespaço das FFAA, o COCiber conta não só com as EPCiber, mas também com os órgãos de ciberdefesa dos Ramos, responsáveis pela resposta a incidentes nos seus CIS. Tendo em conta que os requisitos da capacidade NATO CD DEPLOY podem ser divididos em recursos humanos, devidamente formados, treinados e qualificados, e em recursos materiais, que incluem equipamento informático e de comunicações bem como sistemas de informação e plataformas informáticas, foram também exploradas as capacidades das FFAA Portugueses nestes 2 vetores. Da análise conjugada entre este estudo orgânico da ciberdefesa nacional, dos requisitos mínimos levantados na consecução do OE1, e da análise às entrevistas feitas ao Chefe do COCiber, conclui-se que em relação aos recursos humanos, o CCICE integra a Escola de Ciberdefesa, que faz a formação técnica dos elementos da ciberdefesa, entregues pelos Ramos, permitindo que o COCiber consiga garantir e sustentar a geração de forças de ciberdefesa. Apenas os requisitos *Online Computer Forensic* e *Online Vulnerability Assessment* necessitam de formação adicional para os elementos que operem estas ferramentas informáticas. Focando a questão do treino, manifestado na participação em exercícios, nacionais ou internacionais, de cariz ou com uma componente ciber, como forma de melhorar a proficiência e aumentar a interoperabilidade entre nações aliadas e parceiros, foi identificado que a participação

nestes exercícios está constrangida, desde 2020, por motivos relacionados com a pandemia COVID19. No outro vetor dos requisitos da capacidade NATO CD-DEPLOY, recursos materiais, onde se englobam, todo o hardware, software e CIS, foram identificados 2 requisitos que não se conseguem cumprir, o requisito de possuir um CIS *Security Situation Awareness Decision Support*, que exige que o COCiber possua uma plataforma *Cyber Situational Awareness*, mas as plataformas existentes não possuem ainda o nível de maturidade suficiente. O outro requisito não cumprido está relacionado com o Sistema de gestão de risco, foi identificado que o CCICE possui este tipo de plataformas, mas que necessitam de ajustes de processos para a capacidade CD-DEPLOY. Relativo ao requisito processo lições aprendidas relacionadas com a capacidade de ciberdefesa destacável, este terá que integrar o processo de Lições Aprendidas existente no CACLA.

Respondidas as questões QD1 e QD2, que permitiram atingir os OE1 e OE2, para alcançar o OG "*Propor medidas que permitam que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY)*" e responder à QC "*Que medidas devem ser implementadas que permitam que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY)?*" foram propostas 5 medidas que poderão contribuir para permitir que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY):

MI1) Deve retomar-se a participação regular em exercícios nacionais e internacionais, de cariz ou com uma componente ciber, como forma de consolidar conhecimentos, aumentar a proficiência técnica e desenvolver a interoperabilidade com as nações Aliadas.

MI2) Deve adquirir-se um Sistema de *data labelling and binding*.

MI3) Deve concluir-se o treino dos elementos do COCiber que vão operar as plataformas *Online Computer Forensic* e *Online Vulnerability Assessment*.

MI4) Devem ser efetuados os ajustes necessários aos processos do Sistema de gestão de risco do CCICE, para a capacidade NATO CD-DEPLOY.

MI5) O processo de lições aprendidas associado à capacidade de NATO CD-DEPLOY deve ser integrado no processo de lições aprendidas no CACLA.

Identifica-se como principal **contributo para o conhecimento** a proposta das 5 medidas de implementação para a certificação das FFAA Portuguesas na capacidade de ciberdefesa destacável NATO CD-DEPLOY, que permitem oferecer às nossas forças militares destacadas uma maior proteção.

Este estudo apresenta **limitações**, relacionadas com o facto de grande parte do conhecimento da área de ciberdefesa estar concentrada em poucas pessoas, e concorrentemente, as capacidades de ciberdefesa não serem explicitadas, como forma de dissuasão, para que potenciais adversários não consigam aferir as capacidades reais de ciberdefesa, o que dificulta o acesso a esta informação. Adicionalmente, o ciberespaço é ainda um domínio recente, assim como muitas das capacidades abordadas, não havendo ainda literatura consolidada. Em termos de terminologia, há alguma dificuldade em estabelecer paralelismos entre a doutrina NATO e a realidade nacional, e há alguma diversidade de conceitos, que dificulta o enfoque em determinadas matérias.

Relativamente a **estudos futuros** sugere-se o estudo da orgânica de nações com reconhecidas capacidades em ciberdefesa, e que já possuam a capacidade de ciberdefesa destacável, e a elaboração de doutrina nacional em matéria de DCIS.

Como **recomendações de ordem prática** sugere-se que, a nível de recursos humanos, se retome a participação nos exercícios nacionais e internacionais de cariz ou com um componente ciber, e terminar o treino dos operadores das plataformas de *Online Computer Forensic* e *Online Vulnerability Assessment*. Em termos de recursos materiais, sugere-se a aquisição expedita de um Sistema de *data labelling and binding*.

Referências bibliográficas

CCDCOE. (2022). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn: CCDCOE Publications.

Cooperative Cyber Defence Centre of Excellence. (2022a). Locked Shields [Página online]. Retirado de https://ccdcoe.org/exercises/locked-shields/, em 3 de junho de 2022.

Cooperative Cyber Defence Centre of Excellence. (2022b). Crossed Swords [Página online]. Retirado de https://ccdcoe.org/exercises/crossed-swords/, em 3 de junho de 2022.

Decreto-Lei n.º 136 de 6 de novembro. (2017). *Lei Orgânica do Gabinete Nacional de Segurança*. Lisboa: Governo de Portugal.

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, 3-31. Lisboa: Governo de Portugal.

Defesa Nacional. (2022a). Ciberdefesa [Página online]. Retirado de https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa, em 4 de junho de 2022.

Defesa Nacional. (2022b). O que é o CAIH [Página online]. Retirado de https://www.defesa.gov.pt/pt/pdefesa/CAIH/pt/caih/Paginas/default.aspx, em 4 de junho de 2022.

Decreto-Lei n.º 3 de 16 de Janeiro. (2012). *Lei Orgânica do Gabinete Nacional de Segurança*. Lisboa: Governo de Portugal.

Despacho n.º 13692. (2013). *ORIENTAÇÃO POLÍTICA PARA A CIBERDEFESA*. Lisboa: Ministério da Defesa Nacional.

EMGFA. (2022). *PDMC 3.20 - Doutrina Militar Conjunta para as Operações no Ciberespaço*. Lisboa: EMGFA.

Estado-Maior-General das Forças Armadas. (2018). *Diretiva estratégica do Estado-Maior-General das Forças Armadas 2018-2021*. Lisboa: Ministério da Defesa Nacional.

European Union Military Staff. (2016). *EU Concept on Cyber Defence for EU-led Military Operations and Missions*. Brussels: European External Action Service.

Fernandes, J. P. (2014). *Ciberguerra: Quando a utopia se transforma em realidade.* Vila do Conde: Verso da História.

Jesus, H. F. (2021). CIBERDEFESA – UMA COMPONENTE DE SEGURANÇA. *Revista Militar nº 2631*. Retirado de https://www.revistamilitar.pt/artigo/1545

Joint Chiefs of Staff . (2018). *Joint Publication (JP) - Cyberspace Operations: JP 3.12*. Joint Doctrine Publications.

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

National Institue of Standards and Technology. (2022). Cyber Ranges [Página online]. Retirado de https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf, em 4 de junho de 2022.

NATO Communications and Information Agency. (2016). *Technical Report TR/2016/SPW011047/5.5.1.2 DEPLOYABLE CYBER DEFENCE REFERENCE CAPABILITY*. Hague: NCIA.

North Atlantic Treaty Organization. (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Brussels: NATO Allied Council.

North Atlantic Treaty Organization. (2014). Wales Summit Declaration Press Release 2014-120 [Página online]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_112964.htm, em 16 de março de 2022.

North Atlantic Treaty Organization. (2016a). *Bi-SC Agreed Capability Codes and Capability Statements*. Brussels: NATO Standardization Office.

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

North Atlantic Treaty Organization. (2020). *Allied joint Publication (AJP) – Allied Joint Doctrine for Cyberspace Operations: AJP-3.20*. Brussels: NATO Standardization Office.

North Atlantic Treaty Organization. (2021). *NATO Interoperability Standards and Profiles*. Brussels: NATO Standardization Office.

North Atlantic Treaty Organization. (2022a). Cyber Defence [Página online]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm, em 3 de junho de 2022.

North Atlantic Treaty Organization. (2022b). Cyber Coalition [Página online]. Retirado de https://www.act.nato.int/cyber-coalition, em 3 de junho de 2022.

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

Prucková, M. (2022). Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO. *CCDCOE Library*.

Resolução de Conselho de Ministros n.º 19/2013 de 21 de março. (2013). *Conceito Estratégico de Defesa Nacional*. Lisboa: Governo de Portugal.

Resolução do Conselho de Ministros n.º 92/2019 de 5 de junho. (2019). *Estratégia Nacional De Segurança Do Ciberespaço 2019-2023*. Lisboa: Governo de Portugal.

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

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

Stoltenberg, J. (2018). Speech by Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference. *Cyber Defence Pledge Conference.* Paris.

Stoltenberg, J. (2019). NATO will defend itself. *Prospect*.

Anexo A – Capability Codes and Capability Statements

DEFENCE - Cyber Threats (P.2.7)

Variant Group: Cyber Defence (2 Capability Codes)

Reference Docs: PO(2014)0358, PO(2014)0598, PO(2015)0580, Cyber Defence Pledge at 28, C-M(2002)49-COR11 Enclosure F, AC/322-N(2015)0033, SD Report on DMCCI-MN CD2 Project, PO(2013)0507, MC 0571, MC 0616

VARIANT GROUP COMMON STATEMENTS

VARIANT COMMON DESCRIPTION	
1.01	Capable of applying security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication, and non-repudiation.
COMMON PRINCIPAL STATEMENTS	
2.01	Capable of organizing and operating security measures used for CIS in a way that prevents attacks and faults from happening and/or mitigates their impact, by implementing: boundary protection; endpoint protection; network protection; physical and personnel protection; deception solutions.
2.02	Capable of organising and operating security measures used to protect data in a way that helps prevent data compromise and/or mitigates its impact by implementing: security metadata management; information redaction/sanitization; secure information deleting; assignment and binding of CIS security markings and labels;.
2.03	Capable of supporting data confidentiality, integrity and availability through the use of modular, reprogrammable, interoperable, backwards compatible and releasable (to both non-NATO partners and partners of opportunity) cryptography.
2.04	Capable of maintaining assured security robustness through cryptographic effectiveness and efficiency based on use of latest technology advances, regular updates, integration with Service Management and Control (SM&C) and interoperability testing and assessment capabilities.
2.05	Capable of planning and controlling attributes related to entities and access to CIS services and information, by implementing: 1) identity management (planning identity management, controlling credentials and identities, authentication); 2) Access management (managing access policy, enforce and authorize access).
2.06	Capable of planning and controlling the CIS assets, CIS services, and their configuration by: 1) managing asset inventory; 2) CIS configuration and update management; 3) cryptographic equipment management; 4) effective and efficient federated key management and distribution, including non-NATO partners; 5) service level agreement management.
2.07	Capable of collecting sensor data about all ongoing activities as well as the state of all relevant CIS components in a comprehensive fashion through the use of sensors and the alignment of syntax, reference points, and semantics for that sensor data.
2.08	Capable of detecting malicious activity and faults by analysing sensor data in order to identify malicious and suspicious actions and activities, and determine the meaning and importance of these activities by looking at their local and a global impact by 1) identifying actions (finding, listing and characterizing related sensor data and recognizing actions); 2) identifying activities (finding, listing and characterizing related actions and recognize activities); 3) estimating activities and context.
2.09	Capable of reacting to incidents in order to stop and mitigate their effect in a timely manner by 1) incident management; 2) Decision making process (identifying options, impact, stakeholders, decision makers and coordinating/disseminating decisions; 3) external response coordination; 4) preserve chain of evidence.
2.10	Capable of recovering from a compromise in the CIS's security resulting from an attack or fault by restoring the system and information integrity, the system availability, and the registration of any compromised information by 1) assessing damage and attacks/faults (including malware and failed software assessment); 2) restoring system and information integrity; 3) restoring service availability; 4) registering compromised information.
2.11	Capable of planning risk management; assessing the risk based on analysed threats, values, dependencies, and asset attributes; accrediting through verification of policy compliance and validation of the risk management; planning business continuity; managing the treatment of risk; and communicating the risk to the relevant stakeholders.
2.12	Capable of planning and controlling the trust that can be put in CIS components through the planning of how to manage trustworthiness, the assessment of CIS components and other parties, and the management of trustworthiness treatment and supply chain security.
2.13	Capable of analysing and evaluating the historical and actual effectiveness of CIS Security, as well as the efficiency with which CIS Security is provided.
2.14	Capable of systematically reviewing the way in which a CIS has been operated, including how risk has been managed, in order to help achieve accountability.

2.15	Capable of managing CIS Security requirements, designing CIS Security (by adopting or developing CIS Security models/architectures/designs to design adaptable and resilient CIS), implementing CIS Security (by maintaining secure software, cryptographic CIS Security components and services, and integrating CIS Security components), verifying and validating CIS Security to ensure that the implemented CIS is built in an efficient and adaptive manner, meets the security requirements, functions correctly, and is aligned with high-level security direction and guidance.
2.16	Capable of determining what information is needed for CIS Security, who needs it, and how it will be collected, assessed, and exploited.
2.17	Capable of gathering and receiving CIS Security information from various sources, in particular information about malicious and non-malicious threats and regarding the value of CIS assets, CISs as a whole, and the missions they support.
2.18	Capable of analysing and evaluating collected CIS Security information.
2.19	Capable of ensuring that available CIS Security information is optimally utilized to support CIS Security, through reporting and disseminating it as required in support of other CIS Security capabilities as well as to relevant partners.

Variant Group:	**Cyber Defence**
Capability Code:	**CD-DEPLOY**
Capability Name:	**Deployable Cyber Defence**
Linkage with CRR12:	**New Code**

CAPSTONE CAPABILITY STATEMENTS	
1.01	Capable of independently applying security measures in deployed networks for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication, and non-repudiation.

PRINCIPAL CAPABILITY STATEMENTS	
2.20	Capable of deploying a modular and scalable CD module that can be adapted to the full range of deployable CIS in terms of size, complexity, and geographic distribution.
2.21	Capable of creating a recognised cyber operations picture in a localised time and space to provide commanders with enhanced situational awareness, improved understanding, decision support and enables better delivery of cyber effects.

ENABLING CAPABILITY STATEMENTS	
3.01	Capable of deploying in theatre for operations that cover the entire spectrum of Alliance missions, including high intensity combat operations, and in any environmental conditions.
3.02	Capable of integrating into a deployed CIS Unit.
3.03	Capable of independent team response deployment to provide support to the subordinate units of the supported headquarters in the event of cyber incidents.
3.04	Capable of operating only as part of a larger unit or on an installation from which it may draw logistic support and force protection.
3.05	Capable, on request, of providing support to the protection of critical civilian infrastructure.

Anexo B – List of Essential (green) and Desirable (yellow) Components of CIS Security

Category	Sub-Category	Components	Required Functionality
Prevent	CIS Protection (Boundary Protection)	Firewall	Firewalls to limit the network traffic to a defined and managed set of network ports, applying the least required privilege principle.
		Email Gateway	Email gateway devices which are capable of scanning incoming emails for malicious code, with regularly updated signatures for detecting such code.
		Other Gateways	Gateway devices that scan incoming and outgoing network traffic for malicious code, with regularly updated signatures for detecting such code.
		Behavioural-based mechanisms	Behavioural, and reputation based mechanisms to support the signature-based controls.
		Web content filtering	Measures to implement web content filtering.
	CIS Protection (End-Point Protection)	Endpoint installation controls	Software solutions to control the installation, spread and execution of malicious code, for which the signatures for detection are updated at least once per day.
		Certificate based network access control	Certificate based network access control to limit and control the introduction of devices to the network infrastructure.
	CIS Protection (Transmission Security)	Cryptographic devices	Cryptographic devices to encrypt the network traffic at the network layer, approved in accordance with NATO cryptographic policy, commensurate with the security classification and marking of the information being transmitted.
	CIS Protection (Emission Security)	EMSEC measures	A set of electromagnetic emission security measures commensurate with the risk of exploitation and the sensitivity of the information in accordance with AC/322-D(2007)0036 directives.
	Data Protection	Email Security Marking and Binding	Means to enforce the security marking of outgoing email messages by the sender, through specialized software or features of the email client.
		Read/write permission control	Measures to ensure that removable storage media can only operate at 'read-only' mode, unless specifically authorized otherwise.
		Disk encryption	Measures to enforce full disk encryption on mobile devices, commensurate with the security classification and marking of the information handled therein.
		Data Loss Prevention devices	Network Data Loss Prevention devices deployed on the network boundaries.
		Data Storage Sanitization Device	Device to enable secure erasure of storage media for purpose of downgrading its security classification, in accordance with STANAG 4750.
	Identity and Access Management	Identification and authentication mechanisms	Identification and authentication mechanisms to ensure only authorised users have access to the CIS and the information contained within (should implement multi-factor authentication).

Category	Sub-Category	Components	Required Functionality
		User Account Management	Measures to manage the lifecycle of user, system and application accounts, their creation, use and deletion, applying the least required privilege principle.
	Asset Configuration Management	Security Patches	Security patches to maintain secure configurations for all hardware and software and prevent attackers from exploiting vulnerable systems and services.
		Change control process	Measures to ensure all hardware and software are configured based on approved security baselines, applying a strict change control process and justifying any deviations from approved configurations.
Defend	Monitor	Full packet capture tools	Specialized network appliances that allow 'full packet capture' functionality, triggered by suspicious network activity, to enable detailed post-incident investigation.
	Detect	IDS	Intrusion Detection / Prevention devices that are regularly updated with signatures to detect malicious activity in the networks.
		Incident Reporting mechanisms	Standard procedures and processes for the users of the CIS to report any computer or network anomalies they may notice and their report to be timely assessed.
	Respond	Response Plans and Procedures	Procedures and processes for responding to the different types of cyber incidents including personnel for managing the response and contingency plans for business continuity.
		Forensic Trained Personnel and Procedures	Designated personnel trained in digital forensics procedures, to undertake activities related with the identification, collection and preservation of digital information on security incidents.
	Recover	Remediation Personnel and Procedures	Processes and the required personnel to conduct root cause analysis and identify user mistakes, unpatched vulnerabilities or potential gaps in preventive mechanisms that may have led to the incident in order to negate any future occurrences of the same incident.
Assess	Assess CIS Security	Specialised software and personnel for vulnerability assessment	Specialized software tools to conduct automated vulnerability assessments in addition to manual expert assessment.
	Audit	Security Audits	Periodical security audits to verify that National CIS comply with NATO policies and directives on CIS Security and that the applicable CIS Security controls are correctly implemented and maintained.
Sustain	Educate, train and exercise	Recurrent Training	Implement recurring training for personnel responsible for executing CIS Security activities, potentially leveraging the specialized training options provided by NATO through the organisation's education and training facilities.
	Improve	Lessons learned process	

Category	Sub-Category	Components	Required Functionality
Inform	Collect	SIEM, Log aggregation software	Specialized software (i.e. a Security Incident and Event Management (SIEM) tool and its sub-components for log aggregation) to automatically collect all relevant logs in a central repository to facilitate analysis.
	Analyse	Tools supporting incident analysis	A capability (person or a team) with the required training to conduct the incident analysis activities.
	Report and Sharing	Periodic reporting	Standard procedures and processes to ensure periodical reporting of the information related to security incidents to the risk owners as well as the responsible authority.
		Sharing procedures and mechanisms	Procedures and mechanisms to share with NATO and partnering nations: i. Cyber defence incident information ii. Cyber threat intelligence; iii. Best practices on CIS Security and CD; iv. Mitigation measures addressing most critical vulnerabilities

Apêndice A – Modelo de Análise

Tema	Desenvolvimento da capacidade de Ciberdefesa destacável (NATO CD- DEPLOY)			
Objetivo Geral	Propor medidas que permitam que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY).			
Objetivos Específicos	**Questão Central**	Que medidas devem ser implementadas que permitam que as FFAA Portuguesas se certifiquem na capacidade de ciberdefesa destacável (NATO CD-DEPLOY)?		
	Questões Derivadas	**Conceitos**	**Dimensão**	**Técnicas de recolha de dados**
OE1 Analisar a capacidade de ciberdefesa destacável NATO CD-DEPLOY.	**QD1** Quais os requisitos para a capacidade de ciberdefesa destacável NATO CD-DEPLOY?	Ciberdefesa NATO CD-DEPLOY	Ciberespaço Cibersegurança Legislação NATO	- Análise Documental - Entrevistas semiestruturadas
OE2 Analisar as capacidades das FFAA Portuguesas em matéria de ciberdefesa.	**QD2** Quais as capacidades das FFAA Portuguesas em matéria de ciberdefesa?	Capacidade de ciberdefesa das FFAA Portuguesas	Operações no ciberespaço Orgânica	- Análise Documental - Entrevistas semiestruturadas