O Ciberespaço, a NATO e Portugal – uma Trilogia Inter-relacionada[1]

Helder Fialho Jesus
Capitão-de-mar-e-guerra.

Resumo

Este artigo tem por objetivo analisar a adaptação da NATO aos desafios do ciberespaço, no século XXI, bem como a forma como Portugal o encarou na área da segurança e defesa, no mesmo período. Assim, incidiu-se a investigação nos níveis político, militar e técnico da Aliança Atlântica, de modo a perceber-se a importância do ciberespaço e quais as alterações preconizadas, situação posteriormente estendida a Portugal, tendo em vista conhecer o contributo nacional para a NATO nesta área. Na componente militar foi adotada a metodologia DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability), para efeitos de sistematização e coerência, para ambas as partes. No final apresenta-se de forma sumarizada uma análise e conclusões, mostrando quais as áreas onde Portugal se evidenciou. Efetuou-se, complementarmente, uma análise ao conceito estratégico da NATO, aprovado na Cimeira de Madrid, em 2022, no que ao ciberespaço diz respeito, tendo em vista verificar o alinhamento entre o ciberespaço e as três tarefas estratégicas.

Palavras-chave: NATO; Ciberdefesa; Cibersegurança; Operações no Ciberespaço; Conceito Estratégico.

Artigo recebido: 25.01.2024
Aprovado: 08.04.2024
https://doi.org/10.47906/ND2024.168.02

1 Ao longo do presente artigo, serão empregues as designações originais, em inglês, dos diversos organismos, projetos, iniciativas ou outros, conforme conhecidos na NATO, no sentido de garantir a coerência com o assunto, evitando-se traduções diferenciadas.

Abstract
Cyberspace, NATO and Portugal – an Interrelated Trilogy

This article aims to analyze the adaptation of NATO to the challenges of cyberspace, in the 21st century, as well as the way in which Portugal approached cyberspace in security and defense, in the same period, then making a connection between the two parties. Thus, we focused on the political, military, and technical levels, to understand the importance of cyberspace and the changes adopted, what is the current status in NATO and in Portugal, and what was the national contribution to the Alliance. In the military component, the DOTMLPFI methodology was considered for systematization purposes, for both parties. At the end, analysis and conclusions are briefly presented, pointing out the areas where Portugal stood out. An analysis was also carried out on NATO's Strategic Concept, approved at the Madrid Summit in 2022, regarding cyberspace, with the aim of verifying the coherence between cyberspace and the three strategic tasks.

Keywords: *NATO; Cyber Defence; Cybersecurity; Cyberspace Operations; Strategic Concept.*

1. Introdução

No 75.º aniversário da NATO[2], a sociedade atravessa a sua quarta revolução industrial, conforme Klaus Schwab (2016), presidente do World Economic Forum (WEF), descreve no seu livro com o mesmo título, e que se carateriza por uma Internet omnipresente, com sensores de dimensões cada vez mais diminutas, contudo de maiores capacidades, e pela Inteligência Artificial (IA), permitindo assim a interconexão do mundo físico e virtual. Neste sentido, três elementos são fundamentais, nomeadamente os dados, a informação e a comunicação.

Por sua vez, o ambiente de segurança que se vive está a tornar-se mais imprevisível (Burton e Lain, 2020, p. 3), cujas ameaças podem provir de intervenientes estatais e não estatais, com características assimétricas, onde se incluem os ciberataques e a guerra híbrida, confundindo os limites entre as formas convencionais e não convencionais de conflito, cujos ataques estão a aumentar em velocidade, sofisticação e diversidade (NATO, 2023a).

A relevância do ciberespaço[3], que é um produto do ser humano, começou a ser sentida em finais do século passado, com as oportunidades de desenvolvimento na sociedade, mas também pelos riscos associados. Os assuntos ligados à segurança estão, consequentemente, em evolução contínua e a atual era digital acelerou este processo, à medida que as ameaças se desenvolvem rapidamente e a manutenção das capacidades se torna mais complexa (EDA, 2023, p. 23), aumentando a fragmentação e incerteza.

Complementarmente, o sistema internacional também está em transformação contínua, consequência da evolução tecnológica que se está a verificar no mundo. Esta transformação assenta em três grandes categorias: (1) atores – com o surgimento de atores não estatais; (2) meios – com o surgimento do ciberespaço e de tecnologias disruptivas, onde se insere a IA; e (3) contexto – a perceção de uma crise internacional (Carcelli e Gartzke, 2017), que a COVID-19 e a invasão da Crimeia em 2014, reforçada com a guerra na Ucrânia em 2022, representaram para a sociedade ocidental.

A complexidade e a incerteza que caraterizam as sociedades atuais (UNDP, 2021), obrigam a uma preparação para enfrentar as crises, as quais têm três componentes: ameaça, urgência e incerteza (Boin *et al.*, 2016, p. 5), onde os exercícios são fundamentais para garantir a resiliência. A componente do ciberespaço vai tendo um papel cada vez

2 NATO – North Atlantic Treaty Organization

3 Não existe uma definição consensual a nível internacional para Ciberespaço. Em Portugal está definido como: "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" (ENSC – disponível em https://www.cncs.gov.pt/pt/estrategia-nacional/, a qual é diferente da NATO, apresentada mais à frente.

mais primordial, com o reconhecimento dos níveis de topo de diversas organizações internacionais, como sendo a União Europeia (CYBRID)[4], o G7 (Cyber exercise)[5], o World Bank (CSE)[6] ou a própria NATO (CMX)[7]. Esta última tem-se esforçado para se adaptar e transformar ao mesmo ritmo que a sociedade, tendo apresentado a iniciativa NATO 2030 (NATO, 2021a), que se pretende constituir como uma agenda ambiciosa visando garantir que esta Aliança permanece pronta, forte e unida para uma nova era de aumento de competição global. Nesta está incluída a Transformação Digital da NATO (ACT, 2023), onde para além das alterações tecnológicas está implícita uma mudança cultural e mental, a qual pretende facilitar as Multi-Domain Operations (MDO), visando garantir a interoperabilidade, um maior conhecimento situacional e uma tomada de decisões baseada em dados.

As restruturações organizacionais levadas a cabo pela Aliança aos níveis político, militar e técnico, o desenvolvimento de novas capacidades, as novas necessidades de treino, onde o contexto do ciberespaço[8] é cada vez mais relevante, levam a uma maior cooperação e colaboração intra-NATO, com os Aliados, com a União Europeia (UE) e outros países parceiros, bem como com a indústria e o meio académico. O novo conceito estratégico da NATO (NATO, 2022), aprovado na Cimeira de Madrid de 2022, reforça precisamente a importância do ciberespaço e apresenta um regresso à tradição dos conceitos anteriores a 2010, onde é reafirmado que o objetivo fundamental da NATO é garantir a defesa coletiva das nações aliadas, conforme os princípios fundadores da NATO, consagrados no Tratado de Washington de 1949. Como complemento a este objetivo e ao de garantir a segurança das nações aliadas, são apresentadas as três tarefas principais, sendo elas a dissuasão e defesa, a prevenção e gestão de crises e a segurança cooperativa, e que se podem considerar como o elemento vital da estratégia da NATO.

4 https://data.consilium.europa.eu/doc/document/ST-15870-2017-INIT/en/pdf

5 https://www.ecb.europa.eu/paym/pol/shared/pdf/November_2020-G7-fundamental-elements-of-cyber-exercise-programmes.el.pdf

6 https://documents1.worldbank.org/curated/en/099125002162330340/pdf/P1776920e37f660f70b6640fe108468feb5.pdf

7 https://www.nato.int/cps/en/natohq/news_212527.htm

8 De acordo com o *NATO Glossary of Terms and Definitions*, AAP-06 Edition 2021, têm-se as seguintes definições para alguns dos termos associados ao tema do presente artigo:
Cyber Defence – "The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems".
Cyberspace – "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data".
Cybersecurity – Não existe.

A natureza do ciberespaço exige uma abordagem holística através da unidade de esforços em três níveis: político, militar e técnico. A política de ciberdefesa da NATO de 2021 e o seu plano de ação correspondente, reforçam as atividades nestes níveis e em novembro de 2023, em Berlim, decorreu a primeira NATO Cyber Defence Conference, com a presença de decisores destes três níveis (NATO, 2023a). Assim, também será neste sentido que se desenvolve o presente artigo, na parte respeitante à NATO, a que se juntam outros elementos complementares, relativamente à ciência e à cooperação. Seguidamente, apresenta-se uma forma de olhar para a adaptação de Portugal ao ciberespaço, com ênfase para as áreas da Segurança e Defesa e com elementos do contributo de Portugal junto da NATO, no que ao ciberespaço diz respeito, com ênfase a partir de 2015, data da primeira estrutura nacional de ciberdefesa – o Centro de Ciberdefesa (CCD). Termina com uma breve análise, conclusões e considerações de futuro.

2. NATO

Um elemento que é transversal aos três níveis acima referidos é a arquitetura digital da NATO, sendo esta de uma enorme complexidade, na medida em que tem de responder aos seguintes fatores[9]: (1) ambientes estático e projetável; (2) três níveis de comando (estratégico, operacional e tático); (3) diversos requisitos dos espectros das operações militares, sejam específicos dos domínios de operações (ar, mar, terra, ciberespaço e espaço) ou para o *Command, Control, Communications, Computers, Intelligence, Surveillance, Targeting and Reconnaissance* (C4ISTAR); (4) requisitos diferentes das várias comunidades de utilizadores; (5) a visão e serviços, onde se incluem as camadas de dados, serviços e aplicativos com as respetivas funcionalidades necessárias; (6) redes com diferentes classificações de segurança; e (7) sinergias com outros projetos a fim de evitar "reinventar a roda".

a. Nível Político

A Cimeira de Praga (NATO, 2023a), em 2002, constitui-se como um marco de referência no reconhecimento da importância do ciberespaço ao nível político, tendo o termo *cyber* sido utilizado com uma alusão aos *cyber attacks* na declaração final da cimeira. Ainda neste contexto, o termo *cyberspace* foi utilizado pela primeira vez na Cimeira de 2010, em Lisboa (NATO, 2010a), e só mais tarde, na Cimeira de

9 https://www.ndia.org/-/media/sites/ndia/divisions/international/niag/niag-n_2021_0002_calling_notice_geospatial-data-infrastructure_sdi.ashx

Varsóvia (NATO, 2016), em 2016, passou a ser considerado como um domínio para as operações militares, à semelhança da terra, do ar e do mar. A partir desta, o termo *cyberspace* esteve sempre presente nas declarações formais até à Cimeira de Vilnius (NATO, 2023b) em 2023, com exceção da Cimeira de Madrid (NATO, 2022a), na qual foi aprovado o atual conceito estratégico (NATO, 2022b), mas onde a palavra "ciberespaço" não consta, apesar das alusões às ciberameaças, às ciberdefesas e às atividades neste domínio. A resiliência também recebe um papel proeminente no novo conceito, sustentando a ênfase abrangente na defesa coletiva e nas três tarefas principais.

Relativamente ao ciberespaço, este novo conceito reconhece que é um lugar onde existe uma grande competição, com atores maliciosos que tentam degradar as infraestruturas críticas, interferir com os serviços governamentais, roubar informação e propriedade intelectual, bem como impedir as atividades militares. De notar que são feitas referências à Federação Russa e à China na utilização deste domínio, numa alusão às atividades híbridas. Sobre as três tarefas principais, no contexto da ciberdefesa é estabelecido que: (1) a dissuasão e defesa da NATO é uma postura que se baseia numa combinação adequada das capacidades de defesa nuclear, convencional e antimísseis, sendo complementadas por capacidades nos domínios espaciais e no ciberespaço; que o artigo 5.º do Tratado de Washington pode ser invocado pelo *North Atlantic Council* (NAC), decorrente de um conjunto único ou cumulativo de atividades maliciosas no ciberespaço caso atinjam o nível de um ataque armado. Esta é a tarefa onde se centram a maioria das atividades no ciberespaço, seja no reforço de capacidades, seja para reforço da ciberdefesa, das redes e das infraestruturas; (2) a Segurança Cooperativa releva a parceria estratégica com a União Europeia (UE), que já teve três grandes momentos, sendo eles o da assinatura inicial em 2016, na Cimeira de Varsóvia, de uma declaração conjunta (EP, 2016), pelo Secretário-geral da NATO e pelos presidentes do Conselho Europeu e da Comissão Europeia, em 2018 e mais recentemente em 2023, onde a cooperação e partilha de informação no ciberespaço são elementos preponderantes, assim como o combate às ameaças híbridas e a defesa contra ciberataques; (3) A tarefa de prevenção e gestão de crises não tem qualquer alusão ao ciberespaço nem aos ciberataques.

Importa ainda relevar, ao nível político, mais alguns elementos que mostram a preocupação da NATO com o ciberespaço.

Como primeiros passos organizacionais pode relevar-se, em 2002, a aprovação de um *Cyber Defence Programme*, que contemplava a criação da *NATO Computer Incident Response Capability* (NCIRC). Mais tarde, em 2008, o estabelecimento de uma política de ciberdefesa, aplicada às autoridades políticas, militares e técnicas da NATO, que se estendia às nações Aliadas, bem como a criação da *Cyber Defence Management Authority* (CDMA) para coordenar a ciberdefesa em toda a Aliança, sendo esta posteriormente gerida pelo *Cyber Defence Management Board* (CDMB) (Healey e Jordan, 2014, p. 2).

Em 2010, com a aprovação do anterior conceito estratégico (NATO, 2010b) na Cimeira de Lisboa, o ciberespaço ganhou relevância, pois foi a primeira vez que surgiu a este nível. Mas ainda com um objetivo de desenvolvimento de capacidades para efeitos de prevenir, detetar, defender e recuperar de ciberataques. No fundo para garantir a cibersegurança das redes da NATO e dos países aliados.

Em 2012, a ciberdefesa foi introduzida no *NATO Defence Planning Process* (NDPP) (JAPCC, 2017, p. 3), através de uma identificação e prioritização dos requisitos para o processo de planeamento de defesa.

Na Cimeira de Gales (NATO, 2014), em 2014, foi assumido que o direito internacional é aplicável ao ciberespaço, assim como a decisão de invocar o Artigo 5.º no caso de um ciberataque a ser tomada pelo NAC, caso a caso. Criou-se a *NATO Industry Cyber Partnership* (NCIP), destinada à partilha atempada de informações sobre ciberameaças, permitindo aos participantes melhorar o seu conhecimento situacional, aprovou-se uma *enhanced Cyber Defence Policy*, atualizando a versão então existente de 2011 (CCDCOE, 2018a), onde foi considerado que a ciberdefesa era parte integrante na defesa coletiva da Aliança.

Na cimeira seguinte (NATO, 2016), na cidade de Varsóvia, para além do ciberespaço ter sido considerado como um domínio das operações, os Aliados concordaram em implementar o *Cyber Defense Pledge*, que constitui um compromisso para reforçar e melhorar a segurança das redes e infraestruturas nacionais contra ciberataques. No fundo, visava a cibersegurança destes elementos e a sua resiliência, reafirmando que as obrigações previstas no Artigo 3 do Tratado de Washington também se aplicam às capacidades no ciberespaço. Esta situação foi reforçada na última cimeira, em 2023, em Vilnius, de modo a ser uma questão prioritária. Posteriormente, em fevereiro de 2017, os ministros da defesa aprovaram um *Cyber Defence Action Plan* e um roteiro para implementar o ciberespaço como domínio das operações, visando o aumento da capacidade dos Aliados de trabalharem em conjunto, desenvolverem capacidades e partilharem informação.

Da Cimeira de 2018 (NATO, 2018a), em Bruxelas, verificou-se uma alteração na postura da Aliança face às ameaças no ciberespaço, com a criação de um *Cyberspace Operations Centre* (CYOC) e foi ainda acordada a integração dos efeitos no ciberespaço, fornecidos voluntariamente pelos Aliados, nas operações e missões da Aliança, naquilo que é conhecido como *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA). Ainda em Bruxelas, mas na Cimeira de 2021 (NATO, 2021b), releva-se a nova *Comprehensive Cyber Defence Policy*, o reconhecimento que o CYOC atingiu a sua *Initial Operational Capability* (IOC) e a criação do cargo de *NATO Chief Information Officer* (CIO), no contexto de uma restruturação levada a cabo na sede NATO. Este CIO tem a responsabilidade do desenvolvimento de uma abordagem empresarial para a transformação digital e o fornecimento de capacidades da NATO. Na Cimeira de Vilnius (NATO, 2023b), foi lançada a nova *Virtual Cyber Incident Support Capability*

(VCISC), tendo os Aliados concordado com a *Digital Transformation Implementation Strategy*, a qual visa reforçar a capacidade da Aliança de conduzir Operações Multi-Domínio, promover a interoperabilidade e melhorar o conhecimento situacional.
Ainda no nível político, importa relevar dois pontos: (1) de governação – com o *Cyber Defence Committee* (CDC) (NATO, 2023a), criado em 2014, sendo um órgão subordinado ao NAC com a responsabilidade pela governação e pela política de ciberdefesa. Desempenha um papel fundamental na ligação da política, tal como definida pelo NAC, com os níveis operacional e técnico na NATO. Até 2021, o órgão com responsabilidade pelo planeamento estratégico, direção executiva sobre o tema das redes da NATO e da segurança do ciberespaço na Aliança era o *Cyber Defense Management Board* (CDMB), onde havia uma grande ligação civil-militar e representação nacional (CCDCOE, 2018a). Nesse ano, fruto de uma restruturação na sede da NATO, o CDMB foi extinto, sendo substituído pelo *Senior Executive Group* (SEG); (2) de assessoria – com o *Assistant Secretary General – Innovation, Hybrid and Cyber* (IHC) (NATO, 2024) – o principal conselheiro do Secretário-Geral sobre os desafios emergentes de segurança e as suas implicações para a segurança da Aliança.
De destacar ainda o *Crisis Management Exercise* (CMX) (Got, 2020), exercício que serve para testar os procedimentos de consulta e tomada de decisão da Aliança no nível político-militar estratégico, num cenário civil-militar complexo, em ambiente híbrido, onde se incluem os ciberataques.
Releva-se ainda as palavras do Secretário-geral da NATO quando afirma que: "As we have seen in Ukraine, private companies, such as Microsoft, Amazon and Starlink, have become critical actors in their own right. (…) It is not possible to keep our nations safe without the private sector" (NATO SECGEN, 2023), mostrando a relevância de atores não estatais com poderes únicos e dos quais as sociedades estão cada vez mais dependentes, naquilo a que Joseph Nye (2010) refere como a difusão do poder.
A terminar este ponto apresenta-se o foco (NATO, 2023a) da Aliança para a ciber-defesa, que é a de proteger as suas redes próprias, operar no ciberespaço (missões e operações da NATO), ajudar os Aliados a aumentar a sua resiliência nacional e fornecer uma plataforma para consulta política e ação coletiva.

b. Nível Militar

A principal resposta da NATO na vertente militar, relativamente ao Ciberespaço, ocorreu em 2016, na Cimeira de Varsóvia, quando este foi considerado como um domínio das operações (e não domínio operacional, como às vezes é apresentado): "Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea".

Esta situação revela uma alteração significativa na abordagem deste tema, deixando de ter uma postura meramente "técnica", assente numa dissuasão pela negação (Burton, 2015, p. 13) e orientada para a segurança das suas redes e dos países aliados, para passar a ter também uma postura de "missão" (Bigelow, 2017, p. 6). Assim, esta determinação obrigou a alterações em diversas áreas, desde a política, à estratégia, aos conceitos, às doutrinas e aos procedimentos, bem como ao desenvolvimento de capacidades e capital humano face aos novos desafios.

Após esta decisão, foram elaborados dois documentos fundamentais (JAPCC, 2017), sendo eles o *Roadmap to Implement Cyberspace as a Domain of Operations* e a *Military Vision and Strategy on Cyberspace as a Domain of Operations*, tendo em vista a consecução da orientação política, nomeadamente na integração dos efeitos e da doutrina, assim como na revisão das *NATO Rules of Engagement* (ROE) (Goździewicz, 2019). Naturalmente, surgiu posteriormente o CYOC, no *Supreme Headquarters Allied Powers Europe* (SHAPE)[10], para efeitos de acompanhamento e coordenação da atividade operacional da NATO no ciberespaço, planeamento centralizado, bem como para efeitos de conhecimento situacional (NATO, 2018a). Tendo em conta que a NATO se considera como uma organização defensiva, conforme estabelecido logo no primeiro parágrafo do seu conceito estratégico, ter a iniciativa de criação de efeitos no ciberespaço seria incoerente. Assim, estabeleceu-se o conceito de SCEPVA, para efeitos da integração da criação de efeitos no ciberespaço nas operações e missões da NATO, que são fornecidos voluntariamente pelos Aliados. Aqui importa realçar uma grande diferença relativamente aos outros três domínios (terra, mar e ar) e que tem a ver com a transferência de responsabilidade dos meios/plataformas/unidades das nações para a NATO, aquando da integração destas em missões e/ou operações. Ao contrário do que acontece nos três domínios naturais referidos, no ciberespaço as nações garantem a criação dos efeitos pretendidos pelo Comandante da missão/operação, aquando do planeamento e da execução, mas sem qualquer transferência de autoridade sobre os meios que os criam, mantendo-se estes na alçada das nações. A integração dos diversos domínios de operações militares, onde o espaço também é considerado, conflui para o conceito de MDO, aumentando a complexidade no planeamento, assim como as probabilidades de uma execução mais eficaz e eficiente para se atingirem os objetivos estabelecidos.

As nações têm feito um esforço no sentido de terem uma capacidade no ciberespaço, para fins próprios de soberania, mas também para apoiar a NATO. Assim, e tendo em consideração que o desenvolvimento de uma capacidade assenta em oito vetores *Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Intero-*

10 Quartel General do *Allied Command Operations* (ACO), em Mons (https://shape.nato.int/military_command_structure)

perability (DOTMLPFI) (JALLC, 2016) segue-se esta lógica para apresentar os seus desenvolvimentos na Aliança Atlântica, na componente militar relativa ao ciberespaço:

- ***Doctrine*** – A publicação *Allied Joint Doctrine for Cyberspace Operations* (AJP 3-20) (UKGOV, 2020) constitui-se como a doutrina Aliada para efeitos de planeamento, execução e avaliação das operações no ciberespaço, no contexto das operações Aliadas conjuntas. Aqui, de forma clara, estabelece-se que as atividades no ciberespaço são de dois tipos: (1) Cibersegurança[11], tendo em vista a aplicação de medidas de segurança para a proteção da comunicação, da informação e de outros sistemas eletrónicos, e da informação que é armazenada, processada ou transmitida nesses sistemas no que diz respeito à confidencialidade, integridade, disponibilidade, autenticação e não repúdio; e (2) Operações no Ciberespaço definidas como ações no ciberespaço ou através dele tendo em vista preservar a liberdade de ação amiga neste domínio e/ou a criar efeitos para alcançar os objetivos definidos pelos comandantes. Estes tipos de operações podem ser defensivas, para efeitos de garantir um ciberespaço livre, ou ofensivas de modo a projetar poder para criar efeitos que alcancem objetivos militares. De notar que o termo *Cyber Defence* não faz parte do corpo deste documento, surgindo apenas nas referências e nos acrónimos e abreviaturas. Esta situação pode configurar uma maior dificuldade na taxonomia utilizada pelos diferentes níveis na Aliança, bem como no entendimento e interpretação por parte das nações.
- ***Organization*** – O principal realce vai para o CYOC, o qual tem os seguintes objetivos (Brent, 2019): fornecer conhecimento situacional; planear de forma centralizada as operações e missões da Aliança e proceder ao seu acompanhamento e coordenação. Assim, desempenha um papel central neste domínio, colaborando com diversas entidades, que para efeitos de conhecimento situacional recorrem aos países Aliados, bem como a agências da NATO, nomeadamente aos *NATO Intelligence Fusion Centre* (NIFC), *Allied Command Counter-Intelligence* (ACCI) e *Cyber Threat Assessment Cell* (CTAC). De acordo com o coronel Don Lewis (2019), CYOC *deputy director*, este centro serve como componente de teatro para o ciberespaço, com um paralelismo com os comandos geográficos na cobertura dos seus domínios físicos específicos. Por sua vez fornece aos comandantes aconselhamento neste domínio, apoio ao planeamento e integração de capacidades. De notar uma maior integração de capacidades, agregando o ciberespaço com os *Communication Information Services* (CIS) e a de *Electronic Warfare* (EW).

11 Cyber security: The application of 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.

De notar que a *Allied Command Operations (ACO) Comprehensive Operations Planning Directive (COPD) Version 3.0* (2021) que articula o *Operations Planning Process* (OPP) para os níveis estratégico e operacional da NATO, em apoio ao *NATO Crisis Response Process* (NCRP), estabelece, para o CYOC, o seguinte: ao contrário das forças aéreas, terrestres, navais e de operações especiais, que normalmente executam as suas missões e tarefas ao nível operacional e tático dentro de um teatro de operações, os efeitos do ciberespaço, incluindo os CIS, são muitas vezes planeados e executados a um nível estratégico através de uma função centralizada de *Command and Control* (C2).

- ***Training*** – O exercício *Cyber Coalition* (ACT, 2023b) constitui-se como principal exercício da Aliança tendo por base o ciberespaço, realizando-se numa base anual desde 2008, e reúne organismos NATO, Países Aliados e Parceiros e a União Europeia com um total de cerca de 1000 participantes. É planeado e conduzido pelo *Allied Command Transformation* (ACT) sob os auspícios do *Military Committee* (MC) e tem em vista o reforço da capacidade da Aliança de dissuadir, defender-se e combater ameaças no e através do ciberespaço. A sua realização tem três grandes objetivos: (1) Exercitar os mecanismos existentes de interação entre os participantes para melhorar a colaboração no domínio do ciberespaço; (2) Melhorar a capacidade da Aliança para conduzir operações no ciberespaço, exercitando-se o conhecimento situacional e a partilha de informação sobre o ciberespaço e (3) Identificar lacunas de capacidades, requisitos de formação e validar procedimentos em desenvolvimento, a fim de apoiar o desenvolvimento das operações no ciberespaço e melhorar a educação e formação neste domínio. Importa ainda relevar o exercício *Trident Juncture* (Friedl, 2018), que é um exercício destinado a testar a capacidade da NATO para planear e conduzir uma grande operação de defesa coletiva – desde o treino de tropas ao nível tático, até ao comando de grandes elementos de uma força da NATO. No exercício de 2018 (Wright, 2019, p. 30), a integração do ciberespaço como parte ativa deste tipo de exercícios, em complemento aos outros três domínios, foi um marco assinalável, e que tem continuado nos exercícios seguintes:

  > "The impact of Space and Cyber on JISR continues to drive pace into innovation in the Joint Force Commands and SHAPE."

- ***Material*** – A este nível pretende-se responder à seguinte questão: a NATO tem a tecnologia e os equipamentos necessários para equipar as forças de modo a usar a capacidade de forma eficaz (Kamel e Gallup, 2022, p. 5)? O fator interoperabilidade é aqui preponderante, perante a miríade de companhias que desenvolvem as suas soluções, sejam de *hardware* ou de *software*. Neste sentido, o *NATO Standardization Office* (NSO) (NATO, 2017) tem promulgado *Standard Agreements* (STANAGs) e publicações tendo em vista o desenvolvimento de capacidade de agir em conjunto

de forma coerente, eficaz e eficiente para alcançar os objetivos táticos, operacionais e estratégicos dos Aliados, sendo o *NATO Interoperability Standards and Profiles* (NISP)[12] (ADatP-34) um exemplo, entre muitos. A criação do já referido NCIP vem ao encontro desta necessidade, tornando a ligação entre as empresas e os utilizadores mais facilitada.

- ***Leadership*** – A adoção do ciberespaço enquanto domínio das operações, com o estabelecimento de uma política para a Ciberdefesa, com o desenvolvimento subsequente de doutrina, estratégia, conceitos, procedimentos específicos para o ciberespaço e de forma integrada com os outros domínios, mostra a existência de uma liderança efetiva. Pode ainda referir-se, em específico, o cargo de *Deputy Chief of Staff for Cyberspace* (Blessing, 2021, p. 268), para efeitos de orientação estratégica ao *Supreme Allied Commander Europe* (SACEUR).
- ***Personnel*** – As questões relacionadas com as pessoas constituem um dos elementos mais complexos de resolver, porque exige profissionais com conhecimentos específicos, os quais requerem constante atualização, no contexto de um mercado que é muito concorrente. A necessidade de profissionais ligados ao ciberespaço é uma situação que é transversal a todos os países aliados e à própria NATO e que tem a ver com a existência de pessoas qualificadas em tempo de paz e em tempo de guerra, que os acontecimentos mais recentes no leste da Europa a isto obrigam responder. E foi precisamente sobre este tema que o General Curtis. M. Scaparrotti (SACEUR) fez a sua primeira pergunta na visita ao CCD, em outubro de 2017.
- ***Facilities*** – Para além do NATO HQ e dos dois comandos estratégicos, ACT e *Allied Command Operations* (ACO), que se complementam na definição do ambiente operacional atual e futuro[13], onde as questões do ciberespaço estão englobadas, existem três organismos que têm responsabilidades diretas no que ao ciberespaço diz respeito: (1) O CYOC, anteriormente referido, e (2) dois organismos que resultaram de uma grande transformação levada a cabo na NATO em 2012: (a) a *NATO Communications and Information Agency* (NCIA) (NATO, 2022c), que é o principal fornecedor de serviços de comunicações e informação da NATO, onde a cibersegurança das redes da NATO é uma das suas principais responsabilidades. Neste sentido, faz a gestão de incidentes de cibersegurança de rotina, com uma perspetiva técnica e responde ao CYOC quando existe impacto operacional; (b) o *NATO Communications and Information Support Group* (NCISG) (sd), que tem um trabalho complementar ao da NCI Agency, estendendo as redes estáticas por esta gerida até onde são necessárias operacionalmente para as forças destacadas.
- ***Interoperability*** – releva-se o *NATO Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise (*CWIX) (ACT, sd), que é o maior evento de

12 ADatP-34 (https://live.nisp.nw3.dk/pdf/NISP-Vol1-v15.pdf)
13 https://www.act.nato.int/about/the-command/

interoperabilidade na NATO, na área técnica. Destina-se a desenvolver a capacidade de agir em conjunto, de forma coerente, eficaz e eficiente para alcançar os objetivos dos Aliados e cumpre um amplo espectro de requisitos de validação e verificação de interoperabilidade. Neste evento, que tem lugar anualmente no *Joint Force Training Centre* (JFTC), em Bydgoszcz, na Polónia (JFCT, 2022), a NATO, as nações Aliadas e as nações parceiras testam as suas capacidades de comando e controlo visando a eliminação dos riscos de interoperabilidade como um primeiro passo essencial para missões da NATO. Ao mesmo tempo, o CWIX é um banco de testes para especificações de interoperabilidade que são integradas em capacidades experimentais e de campo, prontas para futuras missões da NATO, onde a ciberdefesa é uma das 19 áreas contempladas.

c. Nível Técnico

A preocupação da NATO relativamente ao ciberespaço surgiu inicialmente na componente técnica. Isto porque eram os técnicos quem tinha de lidar com o assunto, nomeadamente na resolução dos incidentes que surgiam na rede da NATO, quer fossem falhas de operação, avarias ou ciberataques. Como exemplo, a partir de 1998, com as operações da NATO nos Balcãs, os ataques de *Distributed Denial of Service* (DDoS) passaram a ser regularmente sentidos nas redes da Aliança, nomeadamente por *hackers* sérvios, tendo em vista criar disrupção nos sítios e nos servidores de e-mail da NATO (NATO PA, 2009).

A Cimeira de Praga, em 2002, preparou o caminho para se criar o *NATO Computer Incident Response Capability (NCIRC)* em 2002. Decorrente da determinação da Cimeira de 2010 em Lisboa, em 2012 foi então criada a NCIA (NATO, 2023a), como o resultado da integração de vários organismos da *NATO Consultation, Command and Control Organization* (NC3O). A NCIA constituiu-se, assim, como o principal fornecedor destes serviços na Aliança, que incorporou o *NATO Computer Incident Response Capability Technical Centre* (NCIRC-TC), sendo este o órgão responsável pela proteção técnica centralizada no que aos ciberataques dizia respeito e atingindo a sua *Final Operational Capability* (FOC) em 2014. Em 2018, o *NATO Cyber Security Centre* (NCSC) substituiu NCIRC-TC, sendo responsável por todo o ciclo de vida das atividades de cibersegurança da NATO, ao nível da aquisição, manutenção e sustentação, bem como na condução de operações e resposta a Incidentes no ciberespaço. A NCIA (NCIA, sd) conta com uma equipa de 3.000 funcionários civis e militares, distribuídos por 29 localizações, na Europa e na América do Norte. A agência está na linha da frente contra as ciberameaças, protegendo as redes da NATO 24 horas por dia, sete dias por semana. Fornecem também capacidades e serviços que são críticos para a capacidade da NATO de cumprir as suas tarefas principais e trabalha igualmente

em parceria com a indústria, a academia e organizações sem fins lucrativos. Existem ainda as *NATO Cyber Rapid Reaction Teams* (RRT) para ajudar os Aliados em caso de ciberataques, que têm uma prontidão de 24 horas, que atuam quando solicitado e aprovado pelo NAC.

A *Alliance C3 Strategy*[14] constitui-se como mais um marco na adaptação da NATO para dar resposta às necessidades, introduzindo o conceito de *NATO Enterprise*, o qual viria a ser posteriormente definido no *The NATO Enterprise Approach for the Delivery of C3*, e com o desenvolvimento posterior da *NATO Enterprise C&I Vision*, tendo em vista a coerência das capacidades C3 com os serviços de Tecnologia de Informação e Comunicação (TIC).

Em termos de projetos em curso, pode referir-se que, em 2019, foram dados passos muito importantes para a modernização das redes da Aliança (NCIA, 2020), através do programa Polaris, que se constitui como um dos primordiais focos da NCIA, sendo o apoio às operações o principal. Este programa destina-se a consolidar a infraestrutura de TIC da NATO, implementando padrões técnicos modernos, de modo a poder ser gerida centralmente, bem como na adoção de novas formas de trabalhar. Este programa inclui esforços para melhorar a cibersegurança e reduzir os custos de manutenção.

A assinatura de acordos bilaterais é um exemplo das parcerias criadas entre a NATO e a Indústria, no âmbito da NCIP (NCIA, 2018), e que são estabelecidos pela NCIA. Estas parcerias visam a partilha atempada de informações sobre ciberameaças (informação técnica não classificada relacionada com ameaças e vulnerabilidades no contexto do ciberespaço) permitindo melhorar o conhecimento situacional e a proteção das redes. Na prática, facilitará o intercâmbio bilateral rápido e atempado de informações. Como exemplos de entidades têm-se a Microsoft, Fortinet, CISCO, Thales, a Vodafone, a AT&T e a CY4GATE.

No âmbito dos projetos de Smart Defence, no que ao ciberespaço diz respeito, são três os que se apresentam (Cordey e Dewar, 2019, p. 123): (1) O *Multinational Cyber Defence Capability Development* (MNCD2) (NCIA, 2014) e que se destina a facilitar a troca de informações relacionadas a ciberincidentes entre equipas nacionais de *Computer Security Incident Response Teams* (CSIRT), tendo em vista a criação de um "*Cyber Information and Incident Coordination System*"; o (2) *Malware Information Sharing Platform* (MISP) (NATO, 2013), liderado pela Bélgica, e concebido para ajudar na defesa contra ciberataques. Esta plataforma visa facilitar a partilha de informação sobre as características técnicas de *malware*, numa comunidade confiável; e o *MultiNational Smart Defence Project on Cyber Defence Education & Training* (MNCDE&T) (MNCDET, sd), liderado por Portugal (Monteiro, 2017), que se destinava a criar uma Plataforma de Coordenação de Educação e Treino (E&T) de Ciberdefesa e apresentar

14 C-M(2014)0016 – 07April2017.

novas iniciativas visando colmatar as deficiências de E&T de Ciberdefesa das nações aliadas e da NATO. Este projeto terminou em 2019 (DELNATO, 2019), apresentando uma estrutura curricular para a formação de peritos em cibersegurança. Os novos cursos passaram, posteriormente, a ser lecionados nos diferentes países Aliados e Parceiros, bem como na NCI Academy, em Oeiras[15].

A *NCI Academy*, que se estabeleceu formalmente em Oeiras em maio de 2019 (MDN, 2019), encontra-se na dependência da NCIA. A sua localização em Portugal decorreu das alterações aprovadas no seio da NATO quanto à nova orgânica dos seus Comandos, decorrente da Cimeira de Lisboa em 2010, e que determinaram a desativação do *Allied Joint Force Command Lisbon* (JFC Lisbon). No mesmo espaço encontra-se agora a *NCI Academy*, que até então estava sediada em Latina, Itália, com a designação de *NATO CIS School* (NCISS). Incorporou ainda outras entidades independentes de educação e formação individual, como o *NATO Programming Centre*, localizado em Glons e a *NATO Consultation, Command and Control Agency* (NC3A), localizada em Haia. Assim, a *NCI Academy* mantém uma longa tradição de oferta de educação e formação na área de *Consultation, Command, Control, Communications and Intelligence, Surveillance and Reconnaissance* (C4ISR) e do ciberespaço (NCIA, 2022).

Ao nível da governação importa referir pelo menos dois pontos: (1) o *Digital Policy Committee* (NATO, 2023c) – responsável perante o NAC pela assessoria política e técnica em diversas áreas, entre elas a ciberdefesa. Em dezembro de 2023, por decisão do NAC, substituiu o *NATO Consultation, Control and Command Board (NC3B)*, para melhor refletir o seu âmbito e visão, na era digital. Com esta alteração, a NATO considera que vai permanecer na vanguarda dos novos desenvolvimentos tecnológicos, mantendo ao mesmo tempo a interoperabilidade para uma interface perfeita entre os domínios militares e as forças armadas Aliadas; (2) o *Chief of Information Officer* (CIO) (NATO, 2023a) – responsável por garantir a integração, o alinhamento e a coesão dos sistemas e serviços de TIC em toda a NATO e supervisiona o desenvolvimento e a operação das capacidades de TIC. O CIO é também a autoridade para as questões de cibersegurança em toda a NATO, onde se inclui a liderança da gestão de incidentes, a orientação de investimentos específicos nesta área, a melhoria da postura de cibersegurança da Aliança, bem como o aumento da sensibilização em cibersegurança.

15 https://otan.missaoportugal.mne.gov.pt/pt/noticias/ultima-reuniao-do-projeto-multinational-cyber-defence-education-and-training-na-sede-da-nato

d. Complementar

Em complemento aos três níveis acima referidos, identificam-se ainda outras iniciativas que concorrem para a forma como a NATO aborda o ciberespaço. Neste sentido destacam-se:

(1) *NATO Science and Technology Organization* (STO) (STO, sd) – Órgão criado para satisfazer as necessidades coletivas de Ciência e Tecnologia da NATO e dos Aliados, através da partilha e disseminação de conhecimento científico, desenvolvimentos tecnológicos e inovação resultantes de inúmeras atividades suas. Este foi criado em 2012, como resultado da reforma que a NATO levou a cabo nesse ano, o qual reúne a maior rede mundial de investigação em defesa e segurança, reunindo cientistas, engenheiros e analistas nacionais, a indústria e o meio académico para colaborarem no âmbito de um quadro confiável da NATO.
(2) *Science for Peace and Security* (SPS) (NATO, 2023e) – Programa que promove o diálogo e a cooperação prática entre os Estados-membros da NATO e os países parceiros com base na investigação científica, na inovação tecnológica e no intercâmbio de conhecimento. No âmbito deste artigo, as atividades SPS na área da ciberdefesa visam melhorar a sensibilização, o reforço de capacidades, bem como a investigação e o desenvolvimento, sendo exemplos mais recentes o Azerbaijão, a Jordânia, a Tunísia, a Macedónia do Norte, a Mongólia e a República da Moldávia. Com estes dois últimos, a NCIA (NCIA, 2021a.b.) forneceu equipamento, formação e aconselhamento técnico para o estabelecimento de *Cyber Incident Response Capabilities* (CIRC) para as respetivas forças armadas.
(3) *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) – Com a integração da Estónia na NATO, em 2004, este país apresentou o conceito de um centro de excelência internacional para a Ciberdefesa (CCDCOE, sd), o qual foi aprovado pelo *Supreme Allied Commander Transformation* (SACT) em 2006. O CCDCOE foi criado em 2008, com a respetiva acreditação e estatuto de *International Military Organizaton* atribuídos pelo NAC. Atualmente conta com 39 nações (CCDCOE, 2023), sendo 9 delas nações parceiras e tem como missão apoiar os países Aliados e a NATO com conhecimentos interdisciplinares únicos no domínio da investigação, formação e exercícios de ciberdefesa, abrangendo quatro áreas de foco: tecnologia, estratégia, operações e Direito. O *Steering Committee* é o principal órgão de orientação, supervisão e decisão sobre todos os assuntos relativos à administração, políticas e funcionamento do CCDCOE, onde as nações Aliadas integrantes estão representadas. Este centro desenvolveu três grandes produtos: (1) a *International Conference on Cyber Conflict* (CyCon)[16], que teve a sua primeira

16 https://ccdcoe.org/cycon/

edição em 2009, e que tem uma periocidade anual tendo-se tornado um evento de referência na comunidade de profissionais de cibersegurança e ciberdefesa, aderindo aos mais altos padrões de pesquisa académica. Durante três dias, contando com cerca de 600 presenças onde se incluem decisores políticos, líderes de opinião, especialistas em Direito e tecnologia, militares, meio académico e indústria de quase 50 países, são discutidos os atuais desafios de segurança no ciberespaço, de uma forma interdisciplinar; (2) O exercício *Locked Shields*[17], cuja primeira realização ocorreu em 2010, sendo o maior e mais complexo exercício internacional de ciberdefesa. Este exercício técnico expandiu-se consideravelmente ao longo dos anos, simulando toda a complexidade de um incidente massivo no ciberespaço – além da defesa de sistemas informáticos e militares regulares, juntamente com infraestruturas críticas, os especialistas em cibersegurança e ciberdefesa podem praticar a tomada de decisões estratégicas e a comunicação jurídica e mediática, tendo uma periodicidade anual; (3) o *Tallinn Manual*, cujo processo foi lançado em 2009, e que se constitui como uma das realizações de investigação mais conhecidas e reconhecidas internacionalmente para o CCDCOE. A edição original, publicada em 2013, abordava as operações no ciberespaço mais notórias – que têm a ver com o uso da força e o exercício do direito de autodefesa pelos Estados. Em 2017 foi publicado o *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[18], que ampliou a anterior edição, com uma análise jurídica dos incidentes no ciberespaço que ficam abaixo dos limiares do uso da força ou do conflito armado. Apesar deste manual ser uma análise muito abrangente sobre como o Direito Internacional existente se aplica ao ciberespaço, há também quem considere que apresenta uma visão ocidental de abordar esta realidade[19]. Em 2021 foi lançado o projeto para o *Tallinn Manual* 3.0, que envolverá a revisão de capítulos existentes e a exploração de novos temas de importância para os Estados, face às alterações entretanto surgidas desde 2017. Importa ainda relevar duas outras iniciativas do CCDCOE, concretamente o (1) *Cyber Commanders' Handbook* (CCDCOE, 2020) que apresenta linhas de orientação para apoiar o planeamento, coordenação, execução e avaliação das operações no ciberespaço e (2) o exercício *Crossed Swords*[20], que teve a sua primeira edição em 2016, onde são testadas as capacidades e habilidades práticas necessárias ao planeamento e execução de operações ofensivas no ciberespaço.

17 https://ccdcoe.org/exercises/locked-shields/

18 https://ccdcoe.org/research/tallinn-manual/

19 A este respeito é interessante ver "De" colonizando o direito internacional do ciberespaço: a desconsideração da visão latino-americana, publicado pelo *Brazilian Journal of Development*, em 2022, no sítio https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/45756

20 https://ccdcoe.org/crossed-swords/

3. Portugal

Para a salvaguarda do Ciberespaço em Portugal, no contexto da sua proteção, segurança e defesa (conceito PSD) são vários os momentos e os atores que intervêm. Nesta parte, pretende apresentar-se, de forma sintetizada, aqueles que se consideram de maior relevância, com um destaque posterior para a componente militar, pela sua ligação prática e mensurável à NATO.

Assim, em 2013, o *Conceito Estratégico de Defesa Nacional* (CEDN) (RCM, 2013a) e a Reforma "Defesa 2020" (RCM, 2013b) definiram as orientações políticas para a implementação da reforma estrutural na defesa nacional e nas Forças Armadas em 2014/2015. O primeiro ao caraterizar a tipologia das ameaças transnacionais refere que, para responder às ameaças e riscos seria necessário definir, no contexto do ciberespaço, uma estratégia e uma estrutura nacional, a criação de órgãos técnicos necessários; a sensibilização dos operadores públicos e privados para a natureza crítica da segurança informática, assim como levantar a capacidade de ciberdefesa nacional. A segunda reforça este último ponto, estabelecendo a necessidade de se proceder ao levantamento da capacidade de ciberdefesa nacional, como uma das orientações específicas no ciclo de planeamento estratégico. No âmbito desta reforma, e no seguimento da aprovação à primeira alteração à Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA) (AR, 2014) foi aprovada uma nova orgânica do Estado-Maior-General das Forças Armadas (EMGFA) (MDN, 2014), determinando que a estrutura interna do EMGFA seria aprovada por decreto regulamentar. Assim, através do Decreto Regulamentar n.º 13/2015 (MDN, 2015), é criado o Centro de Ciberdefesa. Em 2023, este passou a designar-se por Comando de Operações de Ciberdefesa, através do Decreto Regulamentar n.º 2/2023 (MDN, 2023), que aprova a nova estrutura orgânica do EMGFA, concluindo desta forma a nova reforma da estrutura superior das Forças Armadas iniciada em 2021, com a revisão da Lei de Defesa Nacional e com a aprovação da nova LOBOFA (AR, 2021).

Em 2014 surgiu o Centro Nacional de Cibersegurança (CNCS) (PCM, 2014), na alçada do Gabinete Nacional de Segurança, num trabalho que já vinha desde 2012, e que vem dar robustez à resposta nacional para os incidentes no ciberespaço. Com a publicação do Regime Jurídico da Segurança do Ciberespaço (AR, 2018) é atribuída ao CNCS a competência de Autoridade Nacional de Cibersegurança e ao CERT.PT a de ponto de contacto único internacional para reação a ciberincidentes.

Em 2016 é criada a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) (MJ, 2016), na Polícia Judiciária, sendo a unidade operacional especializada para resposta estrutural, preventiva e repressiva ao fenómeno do cibercrime e do ciberterrorismo[21]. Ainda na área da cibercriminalidade existe, na

21 https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=20161118-mj-pj

Procuradoria-Geral da República, desde 2011, o Gabinete Cibercrime[22] que tem caráter de estrutura de coordenação da atividade do Ministério Público nesta área. Os Serviços de Informações de Segurança (SIS) têm um órgão que trata os assuntos do ciberespaço, onde se integram também as tarefas de combate à ciberespionagem. Em 2016 foi criado o cargo de embaixador para a Ciberdiplomacia[23] e em 2020, em acumulação, o cargo de embaixador para a Diplomacia Digital.

Em Portugal existe uma forma holística de encarar a PSD do ciberespaço, tendo-se constituído em 2018 o G4, que é um grupo informal de caráter operacional, integrando o CNCS, CCD, UNC3T e SIS para efeitos de partilha de informação, conhecimento situacional e coordenação de ações. Naturalmente que em certas circunstâncias existem ligações com outras entidades, fruto das necessidades de resposta.

No início dos anos 2000, as Forças Armadas procuraram criar capacidades próprias para dar uma resposta à segurança das suas redes, situação igualmente ocorrida no meio académico. Em 2002 foi criado o CERT.PT, no âmbito da Rede Ciência, Tecnologia e Sociedade (RCTS) gerida pela Fundação para a Computação Científica Nacional (FCCN), sendo a única equipa de resposta a incidentes de segurança informática em Portugal, e acreditada internacionalmente. Em 2014, o CERT.PT transitou para o CNCS com a criação deste centro que assumiu formalmente a coordenação da resposta nacional a incidentes de segurança informática[24]. Na alçada da FCCN surgiu a Rede Nacional CSIRT[25], em 2008, e que pretende criar em Portugal uma cultura de cibersegurança, de partilha de informação e apoio entre os organismos intervenientes na resposta a incidentes, contando atualmente com cerca de 60 entidades registadas.

Ao nível estratégico, e nas áreas da segurança e defesa[26], releva-se a Estratégia Nacional de Segurança no Ciberespaço (ENSC) (RCM, 2019), que apresenta uma visão integrada do ciberespaço, sendo o documento agregador e enquadrador das restantes áreas específicas, as quais deveriam posteriormente elaborar estratégias setoriais. A ESNC define ciberespaço como um "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação". Nota-se que é mais abrangente do que a apresentada pela NATO, agregando as três camadas do ciberespaço (física, virtual e das pessoas) também assumidas pela NATO, mas não vertidas por esta na sua definição. Também na ENSC está a definição de ciberdefesa, que "consiste na atividade

22 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_da_actividade_de_2012.pdf

23 https://www.c-days.cncs.gov.pt/luis-barreira-de-sousa/

24 https://www.fccn.pt/seguranca/rcts-cert/

25 https://www.redecsirt.pt/

26 Em Portugal foram promulgadas várias estratégias no contexto da sociedade onde a digitalização e o ciberespaço são elementos de base, tais como a Estratégia para a Transformação Digital na Administração Pública, mas que não são objeto de análise neste artigo.

que visa assegurar a defesa nacional no, ou através do, ciberespaço", entre outras. Em 2022 surgiu a Estratégia Nacional de Ciberdefesa (ENCD) (RCM, 2022), clarificando que compete às Forças Armadas a execução de operações no ciberespaço ou através dele, quer sejam de natureza ofensiva ou defensiva, como forma de salvaguardar a defesa dos interesses e valores fundamentais, da ordem constitucional, a soberania e independência nacionais, bem como a integridade do território. No entanto, sendo a ciberdefesa uma área setorial contemplada na ENSC, ao ganhar um estatuto nacional, coloca algumas dúvidas nas linhas orientadoras para uma estratégia nacional de segurança global e de hierarquização dos assuntos a nível nacional.

Na parte militar, destaca-se a Diretiva Estratégica do EMGFA 2018-2021 (EMGFA, 2018), onde a Ciberdefesa é considerada como um dos nove objetivos estratégicos, visando a edificação de uma capacidade de ciberdefesa. Nesta decorrência foi criado um grupo de trabalho, liderado pelo EMGFA e com a participação dos três ramos, para a elaboração de um Plano de Ação, o qual está na base da atual estrutura orgânica do Comando de Operações de Ciberdefesa. A Diretiva Estratégica do EMGFA 2021-2023 (EMGFA, 2021) contempla a criação de uma Escola de Ciberdefesa visando capacitar a área dos recursos humanos.

Como nota final, a terminar esta abordagem macro, salienta-se a criação do *Cyber Academia and Innovation Hub* (CAIH) (PCM, 2023), um projeto de Cooperação Estruturada Permanente (PESCO) da UE que tem a liderança de Portugal, cuja visão é de estabelecer uma ligação entre a dimensão militar e civil da segurança do ciberespaço.

Os factos acima apresentados permitem ver que Portugal tem acompanhado as alterações que se têm verificado a nível internacional, adaptando-se ao quadro estratégico para fazer face às ameaças e riscos à segurança, neste caso, no ciberespaço.

A ligação à NATO ao nível político é efetuada através do Ministério dos Negócios Estrangeiros (MNE), que articula com as restantes entidades nacionais a resposta de Portugal. No caso do tema da Ciberdefesa, Portugal tem respondido ao *Cyber Defence Pledge*, de forma articulada envolvendo o EMGFA, o Ministério da Defesa Nacional (MDN) e o Ministério dos Negócios Estrangeiros (MNE), assim como teve participação em reuniões do CDC e do então CDMB. A participação nacional também se tem feito ao nível do exercício CMX, onde a parte do ciberespaço tem presença cada vez mais assídua, no qual as entidades antes referidas, entre outras, participam nas suas áreas de responsabilidade.

Na ligação ao nível militar, os exemplos a seguir apresentados, seguem igualmente a lógica do DOTMLPFI, para efeitos de coerência e sistematização. Assim:

- **Doutrina** – O Estado-Maior-General das Forças Armadas promulgou o PDMC 3.20 – Doutrina Militar Conjunta para Operações no Ciberespaço, alinhado com o AJP-3.20 e outros documentos doutrinários. Portugal participou ainda ativamente na elaboração do *Cyber Commanders' Handbook*.

- **Organização** – A criação do Centro de Ciberdefesa em 2015 e posteriormente, em 2023, do Comando de Operações de Ciberdefesa, ilustram a adaptação e maturação da resposta nacional às operações militares no ciberespaço. O espírito conjunto está presente desde a primeira hora, inicialmente, com o CCD tendo uma lotação de 10 militares, dos três ramos, numa vertente de proteção das redes da Defesa Nacional. Com o decorrer do tempo, constatou-se que não havia capacidade de resposta para o que seria pretendido para uma componente militar neste domínio, nomeadamente para a realização de operações no ciberespaço. Isto, pela sua complexidade e exigência, em várias áreas, entre elas as de planeamento, de C2, *targetting*, de sincronização, de avaliação, entre outras. A realidade atual já é diferente, com uma estrutura alinhada com as boas práticas das nações Aliadas, e com um incremento em recursos humanos para dar resposta às diversas solicitações, processo este ainda em curso e particularmente exigente, no que aos recursos humanos diz respeito.
- **Treino** – O treino é um elemento fundamental para o adestramento tendo em vista o desenvolvimento de conhecimentos, habilidades e atitudes para um desempenho mais eficiente. Os primeiros exercícios de cibersegurança e ciberdefesa realizados em Portugal foram organizados pelo Exército, através da série CiberPerseu, iniciada em 2012[27] e depois pelo EMGFA, conduzidos pelo Centro de Ciberdefesa, em 2018, através do exercício CyberDEx[28], numa vertente militar. Por sua vez, o CNCS passou a ter, também a partir de 2018, o Exercício Nacional de Cibersegurança[29]. Estes exercícios contribuem igualmente para o desempenho nos Exercícios Cyber Coalition, em que Portugal participa desde 2014, como observador, e desde 2016 de forma permanente. Também no âmbito internacional, Portugal passou a participar no exercício *Locked Shields* em 2018 e no exercício *Crossed Swords* em 2020, ambos da responsabilidade do CCDCOE. Nestes dois exercícios internacionais é criada uma equipa nacional, contando com elementos do EMGFA, que lidera, dos três ramos, do MDN, do CNCS e de outras entidades que tenham interesse e/ou necessidade em participar, num conceito de geometria variável, face aos cenários a jogar. Portugal participa ainda no CWIX, sendo a presença nacional assegurada pelo EMGFA, os três ramos, MDN e empresas nacionais, em função do que se pretende testar, sendo uma ocasião de excelência para se procederem a testes de experimentação, pela diversidade de sistemas presentes. Há a registar a presença nacional nas seguintes *Focus Areas* (FA): *Federated Mission Networking* (FMN), *Cyber Defence* (CD) e *Friendly Force Tracking* (FFT), Communications, GeoMetoc num total de 19 FA em 2023. Em 2024 está prevista a participação nacional em mais duas FA, concretamente *Space* e *LandOps*.

27 https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios/ciberperseu
28 https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios/cyberdex
29 https://www.cncs.gov.pt/pt/exercicio-nacional-ciberseguranca/

- **Material** – A ligação à indústria é um fator relevante nesta área onde a aquisição de equipamentos, plataformas e *software* é exigente e em constante atualização. Assim tem sido, através de empresas nacionais e internacionais, tendo em vista a obtenção das melhores condições para se garantir a segurança das redes, dos ambientes técnicos de treino, através do Cyber Range, e de formação, através da Escola de Ciberdefesa. De relevar também a forma como se procedeu ao alinhamento entre o EMGFA, os três ramos e o MDN nesta área, centralizando-se as aquisições de modo a serem criadas sinergias e um ambiente de trabalho idêntico para todos, facilitando assim o processo administrativo de aquisições, bem como de interoperabilidade e entreajuda.
- **Liderança** – A liderança nacional em atividades NATO, no contexto do ciberespaço, tem pelo menos duas situações de menção: (1) o projeto de *Smart Defence MNCD&ET*, que terminou em 2019 (DELNATO, 2019) e (2) o exercício CWIX, com a liderança da *FA Cyber Defence*, que ocorreu entre 2018 e 2021[30]. Neste período foram realizados testes de interoperabilidade, e exploradas e experimentadas diversas soluções em ciberdefesa, muitas vezes consideradas vanguardistas e inovadoras. Deste trabalho resultou um aumento da confiança por parte do ACT e pelos pares no trabalho desenvolvido, cujo reconhecimento foi várias vezes realçado. O abandono desta liderança foi uma decisão própria.
- **Pessoal** – A colocação de elementos nacionais nas estruturas da NATO, no contexto do presente artigo, cinge-se ao SHAPE, na divisão *J6 Cyberspace* e do NCISG. Fora da estrutura da NATO, mas a esta ligados, os assuntos relacionados com o ciberespaço são acompanhados na sede da NATO, em Bruxelas, tanto na Delegação Portuguesa junto da Organização do Tratado do Atlântico Norte (DELNATO), como na Representação Militar de Portugal junto do Comité Militar da NATO (MILREP).
- **Instalações** – A Estação NATO *Satellite Ground Terminal* (SGT) F12 (AR, 2019), que se encontra na Fonte da Telha e através da qual os serviços de CIS são disponibilizados aos navios da Marinha portuguesa em missões na NATO e a *CIS Support Unit* (CSU) Lisboa, que apoia a SGT-F12 e igualmente a *NCI Academy*.
- **Interoperabilidade** – Em termos técnicos, releva-se a participação no exercício CWIX, bem como a integração no projeto *Smart Defence* MISP.

Na lógica do capítulo anterior, dedicado à NATO, na parte complementar podem referir-se duas situações: (1) STO – Portugal participa em diversos projetos, podendo indicar-se, neste contexto, o *Multi-Domain Quantum Key Distribution (QKD) for Military Usage*, por proposta do Instituto de Telecomunicações. A gestão destas atividades está a cargo da Direção-Geral de Recursos da Defesa Nacional (DGRDN), cuja sensibilização da Base Tecnológica e Industrial de Defesa (BTID) é efetuada pela idD Portugal

30 https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/exercicios/cwix

Defence[31]. (2) CCDCOE – A adesão de Portugal ao CCDCOE (CCDCOE, 2018b), em 2018, constitui-se como um momento de afirmação e demonstração de que existe uma preocupação nacional com este domínio. Este centro conta com a presença de um oficial português em permanência, inicialmente no ramo das operações, passando posteriormente para o ramo da estratégia.
Ao nível técnico, na relação entre as duas partes releva-se todo o apoio e disponibilidade para a criação da NCI Academy, em Oeiras, a qual se encontra na dependência da NCIA.
Uma palavra final sobre a temática do ciberespaço, da ciberdefesa e das operações no ciberespaço para três trabalhos académicos no Instituto Universitário Militar (IUM), designadamente nos cursos de promoção a oficial general (CPOG), onde foi concluído que o ciberespaço deveria passar a ser entendido como plataforma para o desenvolvimento de operações, onde as Forças Armadas portuguesas deveriam atuar, conforme os parâmetros, requisitos e procedimentos da NATO (Honorato *et al*., 2017); a importância da articulação entre a cibersegurança e a ciberdefesa, no contexto da defesa coletiva e na gestão de crises (Coelho, 2018); e a necessidade de criar e operacionalizar, com a maior brevidade possível, uma estratégia militar para o ciberespaço, tendo em vista o desenvolvimento da capacidade de ciberdefesa nacional (Nunes, 2020).

4. Análise e Conclusões

A primeira parte deste artigo explora a evolução do ciberespaço na NATO, incidindo essencialmente nos níveis político, militar e técnico. Em termos globais, a aprovação de um conceito estratégico tem subjacente o surgimento de alterações organizacionais, as quais são significativas, como foram os exemplos decorrentes das Cimeiras de Lisboa (2010) e Madrid (2022). Atualmente encontra-se ainda em fase de implementação um conjunto de mudanças, onde a Transformação Digital é um elemento de referência. Assim, pode considerar-se que a NATO é uma organização aprendente (*learning organization*) à luz do estabelecido por Garvin (1993).
Analisando a estratégia da NATO na vertente do ciberespaço, à luz dos três paradigmas estratégicos, referidos por Couto (2020, pp. 249-250) e Ribeiro (2010b, p. 32), pode dizer-se que: na componente genética, de geração e criação de novos meios, são exemplos as novidades introduzidas com a Transformação Digital em curso ou a criação do CIO; na componente estrutural, de organizar e articular os meios, as alterações efetuadas nas diversas estruturas, sendo exemplos o CDC e o DPC (político), CYOC (militar) e o NCSC (técnico). Na componente operacional, de utilização dos

31 https://www.iddportugal.pt/nato-sto/

meios, tal apenas se aplica na componente de cibersegurança, de defesa das suas redes, visto que as operações no ciberespaço, sejam defensivas ou ofensivas, estão a cargo das nações, através do mecanismo SCEPVA, sendo estas que utilizam os meios.
A postura da NATO perante as ameaças no ciberespaço também se alterou, passando de uma posição de proteção de defesa das suas redes, conforme estabelecido no conceito estratégico de 2010 para uma atitude mais musculada, na versão de 2022. Isto porque o ciberespaço é contemplado na postura de dissuasão e defesa da NATO, a qual se baseia numa combinação de capacidades de defesa nuclear, convencional e antimíssil, complementada por capacidades do espaço e do ciberespaço, sendo considerado um domínio das operações militares. O reforço das capacidades no ciberespaço para aumento da resiliência e a sua ligação à segurança e defesa coletiva, elevam a sua relevância, assim como a alusão a invocar-se o artigo 5.º tendo por base um ciberataque. Relativamente à dissuasão no ciberespaço, este tema tem sido discutido na comunidade académica, não se vendo muito essa abordagem ao nível da NATO, podendo inferir-se que é um assunto classificado. Mas a dissuasão funciona com várias dimensões, sendo uma delas a comunicação, no sentido de chegar aos vários destinatários, para efeitos de balizagem de comportamentos.
Nas três tarefas indicadas no novo conceito estratégico, e já referidas anteriormente, estranha-se a ausência do ciberespaço no que à "prevenção e gestão de crises" diz respeito, podendo até afigurar-se uma contradição. Isto porque as atividades maliciosas no ciberespaço têm um impacto cada vez mais significativo na sociedade, podendo originar crises, onde os países mais desenvolvidos acabam por ser os mais vulneráveis, como os ciberataques à Estónia ocorridos em 2007 constituem um excelente exemplo (Joubert, 2012). Por sua vez, Jamie Shea (2017), anterior *Deputy Assistant Secretary General for Emerging Security Challenges*, refere que o Secretário-geral da NATO considera que um ciberataque pode ser tão devastador quanto um ataque convencional. Por sua vez, na Conferência de Segurança de Munique, em 2018, a *NATO Deputy Secretary General Rose Gottemoeller*, relevou a importância de uma maior cooperação entre a NATO e a UE, onde a componente da gestão de crises e do ciberespaço, foi várias vezes realçada (NATO, 2018b).
E o exemplo que se tem hoje na guerra entre a Federação Russa e a Ucrânia mostra bem isso. Assim, uma alusão ao ciberespaço neste contexto permitiria um entendimento mais global deste tipo de ameaças à sociedade, a qual está cada vez mais digitalizada e dependente desta componente. Até porque a NATO criou as *Rapid Reaction Teams* (RRT), que têm por objetivo prestar assistência às nações ou instalações da NATO em caso de ciberataques[32], o que a acontecer será no contexto de uma crise, que a nação, só por si, não consiga resolver.

32 https://www.nato.int/cps/en/natohq/news_118855.htm

No nível militar, um aspeto que é importante para a ação de comando é a compreensão da gestão do risco (Hutson, 2022), a qual é inerente a esta função, e que no caso do ciberespaço pode apresentar algumas dificuldades, uma vez que este é um novo domínio das operações, sendo transversal e apoiante dos restantes, em relação aos quais já existe um nível de maturidade superior.

Por sua vez, as tensões geopolíticas crescentes que se verificam a nível mundial, obrigam a garantir que os ativos e a infraestruturas de TIC sejam mantidos adequadamente, com as respetivas atualizações regulares, a fim de se garantir a proteção e a segurança contra as ciberameaças, cada vez mais complexas e disruptivas. No entanto, sendo a propriedade destas TIC em grande parte de companhias privadas, aumenta a dependência da NATO e dos Estados destes novos atores cada vez mais poderosos, como o atual conflito na Ucrânia o bem demonstra. Por outro lado, este desenvolvimento tecnológico, onde as MDO são um bom exemplo, assentando em grande parte na utilização e exploração do ciberespaço, pelos meios plataformas e equipamentos, obrigando a uma necessidade de maior interoperabilidade. No campo da taxonomia, pode salientar-se que a expressão "operações militares no ciberespaço" é utilizada pela comunidade operacional, que planeia e executa este tipo de operações, encontrando-se o termo "ciberdefesa" em desuso, o qual é muito utilizado ao nível político. Tal pode verificar-se na publicação doutrinária da NATO, o AJP-3.20, em que o termo *Cyber Defence* não surge no seu corpo. Por outro lado, considerando que esta mesma publicação refere a cibersegurança, e a define de forma consensual com aquilo que é comummente aceite, a ausência do termo *Cybersecurity* do AAP-6 é de estranhar, visto que reflete efetivamente o que a NATO faz para a proteção das suas redes. Esta breve descrição mostra que existe a necessidade de uma clarificação dos conceitos e da sua aplicação.

A análise na parte militar, à luz da metodologia DOTMLPFI, permite uma sistematização dos resultados, onde se releva a doutrina através do AJP-3.20, o exercício *Cyber Coalition* para treino e adestramento, o NCISG para apoio às forças destacadas e na parte da interoperabilidade o exercício CWIX. Na parte técnica destaca-se a criação da NCIA, pela importância que esta tem na proteção das redes da NATO e no apoio às operações, sendo um elemento estrutural para a parte política e militar.

Na segunda parte deste artigo, procurou-se apresentar o que foram os desenvolvimentos ocorridos em Portugal no ciberespaço, nas componentes de segurança e defesa. A promulgação do CEDN, em 2013, foi o primeiro momento que caraterizou a preocupação nacional com o ciberespaço, tendo sido depois promulgada documentação diversa. Portugal acompanhou e foi-se adaptando às alterações que foram surgindo no panorama internacional, tendo ocorrido duas modificações substanciais na área da defesa, concretamente em 2014/15 e 2021/22. A primeira com o surgimento do Centro de Ciberdefesa e depois com a passagem deste para Comando de Operações de Ciberdefesa. De relevar ainda a inclusão da ciberdefesa

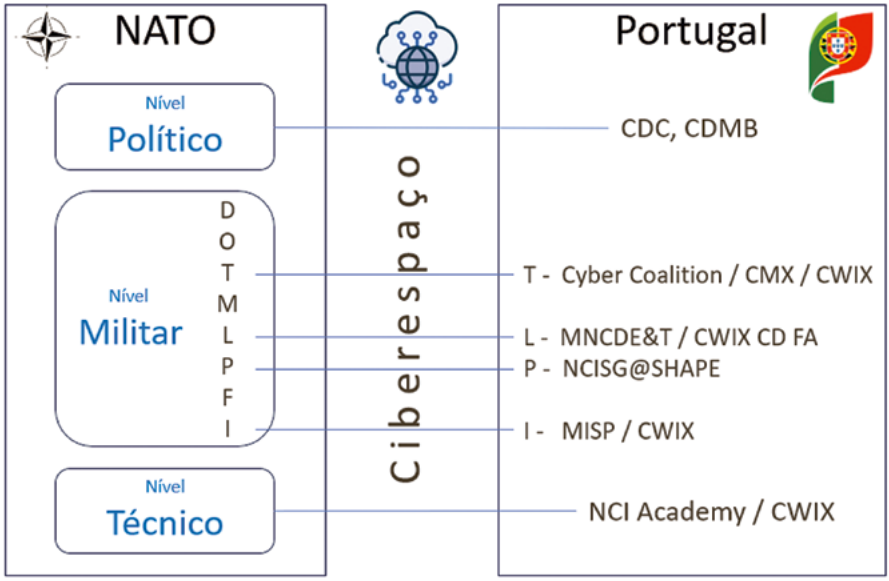
como um dos nove objetivos estratégicos na DEEMGFA 2018-21, que permitiu o foco no desenvolvimento desta capacidade.

Em 2022 foi promulgada a ENCD, alinhada com a ENSC, de 2019, tendo ambas o ciberespaço na sua base. Uma mais geral (ENSC), que engloba a cibersegurança, a ciberdefesa, o combate ao cibercrime, numa postura holística, de orientação e de alinhamento, aguardando-se a posterior promulgação de estratégias setoriais. A outra de caráter setorial (ENCD), para o caso específico da ciberdefesa, a qual pode originar alguns conflitos de análise, no caso de se tentar perceber uma hierarquia estrutural na organização do Estado nesta temática. Por outro lado, tendo em conta a terminologia de Ciberdefesa e Operações no Ciberespaço, seria interessante uma reflexão sobre estes dois termos em dois patamares diferentes, visando uma maior clarificação. Apresenta-se como proposta que o termo Ciberdefesa fique ao nível do MDN, numa vertente política, e as Operações no Ciberespaço ao nível do EMGFA, para a condução deste tipo de operações, à semelhança de outros países, trazendo desta forma maior coerência ao assunto, a que se deveria juntar uma Política para a Ciberdefesa.

Na ligação de Portugal à NATO, no nível político, podem referir-se as participações nas reuniões dos diversos comités e grupos. No nível militar, procurou igualmente seguir-se a metodologia DOTMLPFI, garantindo a coerência de análise. Assim, pode destacar-se, para além das alterações anteriormente referidas ao nível organizacional da ciberdefesa, que seguiram, no geral, as boas práticas internacionais e a elaboração do PDMC 3.20, tendo por referência a doutrina da NATO. Releva-se a participação nos exercícios *Cyber Coalition*, *Locked Shields* e *Crossed Swords*, estes dois últimos da responsabilidade do CCDCOE e, na área da liderança, o projeto de *Smart Defence MNCD&ET*, já concluído e cujo trabalho foi devidamente reconhecido, assim como a liderança portuguesa da *Cyber Defence FA*, do exercício CWIX, entre 2018 e 2021, que também teve o seu reconhecimento, e que poderia ser uma bandeira nacional presente neste 75.º aniversário da NATO. Relativamente à área do pessoal, destaca-se a colocação de um militar no NCISG e a nível da interoperabilidade a participação no MISP. O exercício CWIX, pelas suas características, âmbito e dimensão é transversal a mais de uma área. A NCI Academy, na dependência da NCIA, foi considerada como um contributo nacional no nível técnico.

Em termos finais, pode afirmar-se que a NATO e o ciberespaço, na sua exploração, têm uma relação de um quarto de século, a qual será cada vez mais profunda e dependente, como na maior parte das organizações, e onde Portugal também manterá a sua presença. A NATO continuará a enfatizar a proteção das suas redes e continuará a adaptar as suas políticas, estratégias, conceitos e capacidades no ciberespaço para enfrentar a crescente complexidade das diversas ameaças e desafios. Nestes incluem-se as *Multi Domains Operations*, pela exigência na interoperabilidade, estando o ciberespaço cada vez mais presente na cenarização dos exercícios, bem

Figura 1 – Relação de atividades/áreas de atuação em que Portugal participou de forma efetiva junto da NATO, no contexto do ciberespaço, nos níveis político, militar e técnico



DOTMLPFI – *Doctrine, Organization, Training, Material, Leadership, Personel, Facilities, Interoperability*

como nas questões ligadas à gestão de crises, através dos exercícios da série CMX. As novas tecnologias disruptivas, onde se insere a IA, também se constituem como desafios internos visando o melhor aproveitamento das suas funcionalidades, ou podem constituir-se como ameaças, no caso da sua utilização por parte de atores opositores, num contexto cada vez mais híbrido. Para além do elemento pessoas, o ciberespaço é virtual e físico e não se limita às redes da NATO, pelo que vai exigir novas formas de pensar, de trabalhar e de interagir seja vertical e horizontalmente, bem como interna e externamente, onde a gestão do risco é fundamental para um comandante, face à incerteza predominante. Assim, será reforçada a resiliência desta Aliança e dos países integrantes, através de uma postura robusta, tecnologicamente avançada e cooperativa.

Bibliografia

ACT (2023a). Empowering NATO's Multi-Domain Operations Through Digital Transformation. Disponível em https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/, consultado em 08Jan2024.

ACT (2023b). NATO Exercises to Enhance its Cyber Resilience & Exercise Cyber Coalition. Disponíveis em https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/; e https://www.act.nato.int/activities/cyber-coalition/, consultados em 09Jan2024.

ACT (2023b). NATO Exercises to Enhance its Cyber Resilience & Exercise Cyber Coalition. Disponíveis em https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/; e https://www.act.nato.int/activities/cyber-coalition/, consultados em 09Jan2024.

ACT (sd). Coalition Warrior Interoperability Exercise-CWIX. Disponível em https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise/, consultado em 10Jan2024.

AR (2014). Lei Orgânica n.º 6/2014 – Lei Orgânica de Bases da Organização das Forças Armadas, Assembleia da República (AR). Disponível em https://diariodarepublica.pt/dr/detalhe/lei-organica/6-2014-56384929, consultado em 12Jan2024.

AR (2018). Lei n.º 46/2018 – Estabelece o regime jurídico da segurança do ciberespaço, Assembleia da República (AR). Disponível em https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384, consultado em 12Jan2024.

AR (2019). Resolução da Assembleia da República n.º 221/2019 – Estatuto da NCIA em Portugal, Assembleia da República (AR). Disponível em https://files.diariodarepublica.pt/1s/2019/11/21400/0000700038.pdf, consultado em 13Jan2024.

AR (2021). Lei Orgânica n.º 2/2021 – Lei Orgânica de Bases da Organização das Forças Armadas, Assembleia da República (AR). Disponível em https://diariodarepublica.pt/dr/detalhe/lei-organica/2-2021-169256653, consultado em 12Jan2024.

Bigelow, B. (2017). Mission Assurance: Shifting the Focus of Cyber Defence. 9th International Conference on Cyber Conflict – Defending the Core. NATO CCD COE Publications, Tallinn. Disponível em https://ccdcoe.org/uploads/2018/10/Art-03-Mission-Assurance-Shifting-the-Focus-of-Cyber-Defence.pdf, consultado em 10Jan2024.

Blessing, J. (2021). Fail-Deadly, Fail-Safe, and Safe-to-Fail: The Strategic Necessity of Resilience in the Cyber Domain. Project MUSE. Brookings Institution Press, pp. 261-288. Disponível em https://muse.jhu.edu/pub/11/oa_edited_volume/chapter/3103404, consultado em 10Jan2024.

Boin, A., Hart, P., Stern, E., Sundelius, B. (2016). *The Politics of Crisis Management*, 2nd Edition. Cambridge University Press. https://doi.org/10.1017/9781316339756

Brent, L. (2019). NATO's Role in Cyberspace. Disponível em https://www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/NATOCyberspace.pdf, consultado em 06Jan2024.

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, *Defence Studies*, 15:4, 297-319, DOI: 10.1080/14702436.2015.1108108.

Burton, J. e Lain., C (2020). Desecuritising cybersecurity-Towards a societal Approach. Tailor and Francis Group. https://doi.org/10.1080/23738871.2020.1856903. Disponível em https://www.tandfonline.com/doi/abs/10.1080/23738871.2020.1856903, consultado em 10Jan2024.

Carcelli, S. e Gartzke, E. (2017). The Diversification of Deterrence: New Data and Novel Realities. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.745. Disponível em https://oxfordre.com/politics/display/10.1093/acrefore/9780190228637.001.0001/

acrefore-9780190228637-e-745?d=%2F10.1093%2Facrefore%2F9780190228637.001.0001%-2Facrefore-9780190228637-e-745&p=emailAofSHchKzpCMs, consultado em 09Jan2024.

CCDCOE (2018a). The North Atlantic Treaty Organization (NATO). Disponível em https://ccdcoe.org/organisations/nato/, consultado em 06Jan2024.

CCDCOE (2018b). Portugal to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. Disponível em https://ccdcoe.org/news/2018/portugal-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn/, consultado em 13Jan2024.

CCDCOE (2020). Cyber Commanders' handbook. NATO CCDCOE publications. Tallinn.

CCDCOE (2023). The NATO CCDCOE welcomes new members Iceland, Ireland, Japan, and Ukraine. Disponível em https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/, consultado em 12Jan2024.

CCDCOE (sd). About us. Disponível em https://ccdcoe.org/about-us/, consultado em 12Jan2024

Coelho, J. (2018). O Ciberespaço na Defesa Coletiva e na Gestão de Crises: Articulação entre a Cibersegurança e a Ciberdefesa. Lisboa: Instituto Universitário Militar (IUM). Disponível em https://comum.rcaap.pt/bitstream/10400.26/24522/1/TII_CMG_SCoelho.pdf, consultado em 12Jan2024.

Cordey, S e Dewar, R. (2019). National Cybersecurity and Cyberdefense Policy Snapshots. Disponível em https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_2.pdf, consultado em 11Jan2024.

Couto, A. (2020). *Elementos de Estratégia – Apontamentos para um curso* – Vol I. Fundação Casa Carvalho Cerqueira. Leya.

DELNATO (2019). Última reunião do Projeto "Multinational Cyber Defence Education and Training" na sede da NATO. Disponível em https://otan.missaoportugal.mne.gov.pt/pt/noticias/ultima-reuniao-do-projeto-multinational-cyber-defence-education-and-training-na-sede-da-nato, consultado em 11Jan2024.

EDA (2023). Enhancing EU Military Capabilities Beyond 2040. Disponível em https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities--beyond-2040.pdf, consultado em 09Jan2024.

EMGFA (2018). Diretiva Estratégica do EMGFA 2018-2021. Disponível em https://www.emgfa.pt/Documents/2019/DiretivaEstrategicaEMGFA-2018-2021_Ver.2.pdf, consultado em 12Jan2024.

EMGFA (2021). Diretiva Estratégica do EMGFA 2021-2023. Disponível em https://www.emgfa.pt/Documents/2022/DIRETIVA%20ESTRAT%C3%89GICA%20EMGFA_2021-2023%20-%20Copy.pdf, consultado em 12Jan2024.

EP (2010). NATO Defending against cyber attacks. European Parliament. Disponível em https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf, consultado em 08Jan2024.

EP (2016). EU-NATO Joint Declaration, 8 July 2016, Warsaw. European Parliament. Disponível em https://www.europarl.europa.eu/delegations/en/dnat/documents/eu-texts, consultado em 08Jan2024.

Friedl, M. (2018). U.S. Joins NATO's Trident Juncture Exercise. US DoD. Disponível em https://www.defense.gov/News/News-Stories/Article/Article/1666272/us-joins-natos-trident-juncture-exercise/, consultado em 09Jan2024.

Got, A. (2020). NATO crisis management exercises: preparing for the unknown. Disponível em https://www.nato.int/docu/review/articles/2020/02/07/nato-crisis-management-exercises-preparing-for-the-unknown/index.html, consultado em 09Jan2024.

Goździewicz, W. (2019). Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA). *Cyber Defense Magazine*. Disponível em https://www.cyberdefensemagazine.com/sovereign-cyber/, consultado em 13Jan2024.

Grossman, T. (2023). Cyber Rapid Response Teams Structure, Organization, and Use Cases. Center for Security Studies (CSS), ETH Zürich, disponível em https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2023-11-Cyber-Rapid-Response-Teams.pdf, consultado em 12Jan2024.

Healey, J., Jordan, K. (2014). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow. Atlantic Council – Brent Scowcroft Center On International Security, Washington. Disponível em https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf, consultado em 19an2024.

Honorato, M., Santos, L., Mateus, R. (2017). O ciberespaço como 5.º domínio operacional – Impacto estratégico na Política de Defesa Nacional. Lisboa: Instituto Universitário Militar (IUM). Disponível em https://comum.rcaap.pt/bitstream/10400.26/21956/1/07_TIG%20AEE%20-%20Ciberespa%C3%A7o%205%C2%BA%20Dominio%20de%20Opera%C3%A7%C3%B5es.pdf, consultado em 11Jan2024.

Hudson, P. (2022). Managing Cyber Risk to Mission at the Operational Level. The Three Swords 38/2022, pp 68-71. Joint Warfare Centre (JWC). Disponível em https://www.jwc.nato.int/application/files/1416/7092/6318/CyberRisktoMission_2022.pdf, consultado em 14Jan2024.

JALLC (2016). Joint Analysis Handbook 4th Edition. Disponível em https://www.jallc.nato.int/application/files/9416/0261/6056/Joint_Analysis_Handbook_4th_edition.pdf, consultado em 05Jan2024.

JAPCC (2017). NATO Joint Air Power and Offensive Cyber Operations. Joint Air Power Joint Air Competence Centre. Kalkar-Germany. Disponível em https://www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf, consultado em 10Jan2024.

JFCT (2022). CWIX 2022 poised to deliver a more interoperable, innovative Alliance. Disponível em https://www.jftc.nato.int/articles/cwix-2022, consultado em 10Jan2024.

Joubert, V. (2012). Five years after Estonia's cyber attacks: Lessons learned for NATO? NDC. Disponível em https://www.files.ethz.ch/isn/143191/rp_76.pdf

Kamel, M. e Gallup, S. (2022) Quantifying, Visualizing, and Tracking Capability Gaps. Naval Postgraduate School, Naval Research Program. Disponível em https://apps.dtic.mil/sti/pdfs/AD1184027.pdf, consultado em 09Jan2024.

Lewis, D. (2019). What is NATO really doing in Cyberspace? Texas National Security Review, Disponível em https://warontherocks.com/2019/02/what-is-nato-really-doing-in-cyberspace/, consultado em 08Jan2024.

MDN (2014). Decreto-Lei n.º 184/2014 – Lei Orgânica do Estado-Maior General das Forças Armadas, Ministério da Defesa Nacional. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/184-2014-65983261, consultado em 12Jan2024.

MDN (2015). Decreto Regulamentar n.º 13/2015 – Estrutura Orgânica do Estado-Maior General das Forças Armadas, Ministério da Defesa Nacional. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-regulamentar/13-2015-69920325, consultado em 12Jan2024.

MDN (2019). Portugal entrega formalmente escola da NATO que pretende responder aos desafios da Ciberdefesa e Cibersegurança. Disponível em https://www.defesa.gov.pt/pt/comunicacao/noticias/Paginas/Portugal-entrega-formalmente-escola-da-NATO-que-pretende-responder-aos-desafios-da-Ciberdefesa-e-Ciberseguran%C3%A7a.aspx, consultado em 11Jan2024.

MDN (2023). Decreto Regulamentar n.º 2/2023 – Estrutura Orgânica do Estado-Maior General das Forças Armadas, Ministério da Defesa Nacional. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-regulamentar/2-2023-214042394, consultado em 12Jan2024.

MJ (2016). Decreto-Lei n.º 81/2016 – Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica. Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/81-2016-105263934, consultado em 12Jan2024.

MNCDET (sd). Multinational Cyber Defence Education and Training Project (MN CD E&T). Disponível em https://mncdet.wixsite.com/mncdet-nato, consultado em 11Jan2024.

Monteiro, A. (2017) Portugal at Forefront of Global Cyber Initiatives. AFCEA – Signal – Cyber Edge. Disponível em https://www.afcea.org/signal-media/cyber-edge/portugal-forefront-global-cyber-initiatives, consultado em 11Jan2024.

NATO (2010a). Lisbon Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_68828.htm, consultado em 04Jan2024.

NATO (2010b). Strategic Concept 2010. Disponível em https://www.nato.int/cps/en/natohq/topics_82705.htm, consultado em 04Jan2024.

NATO (2013). Sharing malware information to defeat cyber attacks. Disponível em https://www.nato.int/cps/en/natolive/news_105485.htm, consultado em 11Jan2024.

NATO (2014). Wales Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_112964.htm, consultado em 04Jan2024.

NATO (2016). Warsaw Summit Communiqué. Disponível em https://www.nato.int/cps/en/natohq/official_texts_133169.htm, consultado em 04Jan2024.

NATO (2017). NATO Standardization Office (NSO). Disponível em https://www.nato.int/cps/en/natohq/topics_124879.htm, consultado em 08Jan2024.

NATO (2018a). Brussels Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_156624.htm, consultado em 05Jan2024.

NATO (2018b). Panel Discussion – ''Defence Cooperation in the EU and NATO: More European, More Connected, More Capable?'' Disponível em https://www.nato.int/cps/en/natohq/opinions_152237.htm?selectedLocale=en, consultado em 14Jan2024.

NATO (2021a). NATO 2030-Making A Strong Alliance Even Stronger. Disponível em https://www.nato.int/nato2030/, consultado em 06Jan2024.

NATO (2021b). Brussels Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/news_185000.htm, consultado em 05Jan2024.

NATO (2022a). Madrid Summit Declaration. Disponível em https://www.nato.int/cps/en/natohq/official_texts_196951.htm, consultado em 04Jan2024.

NATO (2022b). Strategic Concept. Disponível em https://www.nato.int/cps/en/natohq/topics_210907.htm, consultado em 04Jan2024.

NATO (2022c). NATO Communications and Information Agency (NCI Agency). Disponível em https://www.nato.int/cps/en/natohq/topics_69332.htm, consultado em 07Jan2024.

NATO (2023a). Cyber defence. Disponível em https://www.nato.int/cps/en/natohq/topics_78170.htm, consultado em 04Jan2024.

NATO (2023b). Vilnius Summit Communiqué. Disponível em https://www.nato.int/cps/en/natohq/official_texts_217320.htm, consultado em 04Jan2024.

NATO (2023c). Digital Policy Committee (DPC). Disponível em https://www.nato.int/cps/en/natohq/topics_69279.htm, consultado em 11Jan2024.

NATO (2023d). Science for Peace and Security Programme. Disponível em https://www.nato.int/cps/en/natohq/topics_85373.htm, consultado em 11Jan2024.

NATO (2024). Principal officials. Disponível em https://www.nato.int/cps/en/natohq/who_is_who_51639.htm, consultado em 09Jan2024.

NATO PA (2009). NATO and Cyber Defence. NATO Parliamentary Assembly. Disponível em 2009 – 173 DSCFC 09 E BIS – CYBERDEFENCE – MYRLI REPORT.doc (live.com), consultado em 11Jan2024.

NATO SECGEN (2023). Speech by NATO Secretary General Jens Stoltenberg at the first annual NATO Cyber Defence Conference. Disponível em https://www.nato.int/cps/en/natohq/opinions_219806.htm, consultado em 9Jan2024.

NCIA (2014). MN CD2 Nations release tool to share cyber incident information. Disponível em https://www.ncia.nato.int/about-us/newsroom/mn-cd2-nations-release-tool-to-share-cyber-incident-information.html, consultado em 11Jan2024.

NCIA (2018). New NATO-Industry cyber partnerships signed at NITEC18. Disponível em https://www.ncia.nato.int/about-us/newsroom/new-natoindustry-cyber-partnerships-signed-at-nitec18.html, consultado em 11Jan2024.

NCIA (2020). NATO Platform to lay the foundations for services, apps and agility. Disponível em https://www.ncia.nato.int/about-us/newsroom/nato-platform-to-lay-the-foundations-for-services--apps-and-agility.html, consultado em 11Jan2024.

NCIA (2021a). NATO assists Mongolia in bolstering its cyber security posture. Disponível em https://www.ncia.nato.int/about-us/newsroom/nato-assists-mongolia-in-bolstering-its-cyber-security-posture.html, consultado em 11Jan2024.

NCIA (2021b). NATO assists Moldova in improving its cyber security capabilities. Disponível em https://www.ncia.nato.int/about-us/newsroom/nato-assists-moldova-in-improving-its-cyber-security-capabilities.html, consultado em 11Jan2024.

NCIA (2022). Introducing the NATO Communications and Information Academy. Disponível em https://www.ncia.nato.int/resources/site1/general/what%20we%20do/nci%20academy/nci_academy_brochure_web_2022_sep.pdf, consultado em 11Jan2024.

NCIA (sd). Who we are. Disponível em https://www.ncia.nato.int/about-us/who-we-are.html, consultado em 11Jan2024.

NCISG (sd). About us – NATO Communications and Information Support Group. Disponível em https://ncisg.nato.int/about-us, consultado em 10Jan2024.

Nunes, P. (2020). A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço. Coleção "ARES", 36. Lisboa: Instituto Universitário Militar (IUM). Disponível em https://www.ium.pt/pub/65, consultado em 11Jan2024.

Nye, Joseph (2010). *Cyber Power*. Belfer Center for Science and International Affairs | Harvard Kennedy School.

PCM (2014). Orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança (CNCS). Disponível em https://files.diariodarepublica.pt/1s/2014/05/08900/0271202719.pdf, consultado em 11Jan2024.

PCM (2023). Decreto-Lei n.º 34/2023 – Cyber Academia and Innovation Hub (CAIH). Disponível em https://diariodarepublica.pt/dr/detalhe/decreto-lei/34-2023-213345452, consultado em 12Jan2024.

RCM (2013a). Conceito Estratégico de Defesa Nacional (CEDN). Resolução do Conselho de Ministros n.º 19/2013. Disponível em https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf, consultado em 12Jan2024.

RCM (2013b). Reforma "Defesa 2020". Resolução do Conselho de Ministros n.º 26/2013. Disponível em https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Defesa-2020.pdf, consultado em 12Jan2024.

RCM (2019). Estratégia Nacional de Segurança no Ciberespaço (ENSC). Resolução do Conselho de Ministros n.º 92/2019. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/92-2019-122498962, consultado em 12Jan2024.

RCM (2022). Estratégia Nacional de Ciberdefesa (ENCD). Resolução do Conselho de Ministros n.º 92/2019. Disponível em https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924, consultado em 12Jan2024.

Ribeiro, A. (2010). *Teoria Geral da Estratégia – O essencial ao processo estratégico*. Coimbra: Almedina,

Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.

Shea, J. (2017). Cyberspace as a Domain of Operations. What Is NATO's Vision and Strategy? Disponível em https://apps.dtic.mil/sti/pdfs/AD1068701.pdf, consultado em 10Jan2024.

STO (sd). About the NATO Science and Technology Organization (STO). Disponível em https://www.sto.nato.int/Pages/default.aspx, consultado em 11Jan2024.

UK Gov (2020). Allied Joint Doctrine for Cyberspace Operations (AJP-3.20). Disponível em https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320, consultado em 05Jan2024.

UNDP (2021). UNDP's Strategic Plan 2022-2025: Designing for Complexity and Uncertainty. Disponível em https://www.undp.org/future-development/blog/undps-strategic-plan-2022-2025-designing-complexity-and-uncertainty, consultado em 09Jan2024.

Wright, N. (2019). Some Lessons From Command Post Exercise Trident Juncture 2018. Joint Warfare Centre (JWC)- The Three Swords Magazine, Stavanger Disponível em https://www.jwc.nato.int/application/files/4116/4680/4222/issue34.pdf, consultado em 09Jan2024.