ESCOLA NAVAL

talanteobfaire

Departamento de Ciências do Mar

Filipa Couto Astorga Batista Pinto

Enquadramento Técnico-Jurídico da Segurança do Ciberespaço

Aplicabilidade na Marinha

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Alfeite

2019

ESCOLA NAVAL

talant de bien faire

Filipa Couto Astorga Batista Pinto

Enquadramento Técnico-Jurídico da Segurança do Ciberespaço
Aplicabilidade na Marinha

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha

Orientação de: Ana Sofia Nunes Rodrigues da Silva Vaz Geraldes

Coorientação de: CTEN EN-AEL Mário Rui Monteiro Marques

O Aluno Mestrando

O Orientador

Alfeite

2019

Epígrafe

The weakest link of security is people.

(Mitnick e Simon, 2002)

Dedicatória

Aos meus pais e aos meus irmãos que desde sempre e à sua maneira me ensinaram o valor da vida e a conquistar cada passo do meu futuro,

Aos meus amigos que se mantiveram ao meu lado e me ajudaram a percorrer este percurso,

Um profundo obrigado.

Agradecimentos

Gostaria de agradecer a todos os que me auxiliaram e de alguma forma contribuíram para a realização da minha dissertação de mestrado, disponibilizando o seu tempo e a sua atenção, nomeadamente:

À minha orientadora, Ana Sofia Nunes Rodrigues da Silva Vaz Geraldes, um especial obrigado que incansável e prontamente me auxiliou e acompanhou no desenvolvimento da minha dissertação;

Ao meu coorientador, Sr. º Engenheiro Mário Rui Monteiro Marques, por coorientar a minha dissertação;

Ao Sr. º Almirante Gameiro Marques (GNS/CNCS); aos Srs. º Comandantes Fialho Jesus (CCD), Baptista das Neves (NCIRC Marinha), Courela Alexandre (NCIRC Marinha) e Caldeira Carvalho (EMA); aos Srs. º Engenheiros Câmara da Assunção (CCD) e Marques Prates (EMA) e, por fim, à Sr.ª Tenente Inês Silva (DJOI), pela pronta disponibilidade em esclarecerem as minhas dúvidas e partilharem comigo os seus conhecimentos.

Resumo

O ciberespaço é um domínio com características particulares, onde a ausência de fronteiras físicas, a fácil acessibilidade, a anonimidade de ação, a independência temporal e espacial e a conexão à imensidão de serviços de uma nação, o tornam num espaço de dois gumes.

Este espaço virtual permitiu um abrupto crescimento e desenvolvimento económico notório nos Estados, empresas e organizações, permitindo e facilitando ainda muitas das tarefas e atividades dos cidadãos. Os seus benefícios originaram uma maior aderência e dependência às suas utilidades. Contudo, a mesma dependência, especialmente dos serviços vitais de cada Estado, torna-os vulneráveis às ameaças do ciberespaço.

A interligação das redes e sistemas de informação e comunicação, concede-lhes um maior comprometimento dos mesmos e inerentemente, de todos os serviços a que estão associados. Neste sentido, diversas entidades têm realizado esforços para garantir a segurança dos mesmos e prevenir a ocorrência de incidentes cibernéticos.

Deste modo, Portugal têm concorrido com inúmeras medidas e atividades, nas quais se inclui mais recentemente a Estratégia Nacional de Segurança do Ciberespaço, que define uma estratégia de ação na vertente da segurança do ciberespaço, e a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço. A NATO e a União Europeia são duas organizações que Portugal integra e onde se destaca a sua envolvência no tema abordado e nas colaborações realizadas com o país.

Considerando o atual paradigma e a relevância deste tema, o presente trabalho integra as capacidades que a Marinha Portuguesa possui neste âmbito, analisando-as através da abordagem DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade) da NATO.

Palavras-chave: ciberdefesa, ciberespaço, cibersegurança, Estratégia Nacional de Segurança do Ciberespaço, Marinha Portuguesa.

Abstract

Cyberspace is a domain with particular characteristics, where the absence of physical boundaries, easy accessibility, anonymity of action, temporal and spatial independence and the connection to the vastness of nations services make it a two-edged space.

This virtual space allowed for an abrupt growth and notorious economic development in states, companies and organizations, allowing and facilitating many of the tasks and citizens activities. Its benefits have led to a greater adherence and dependence on its utilities. However, this same dependence, especially on vital services of each state, makes them vulnerable to cyberspace threats.

The interconnection of networks and information and communication systems gives them a greater commitment of the same and inherent, of all the services to which they are associated. Therefore, several entities have made efforts to ensure their security and prevent the occurrence of cyber incidents.

Thus, Portugal has been involved in several measures and activities, most recently including the National Cyberspace Security Strategy, which defines a strategy on cyberspace security, and Law No. 46/2018, of 13 August, which establishes the legal regime of cyberspace security. NATO and the European Union are two organizations where Portugal is integrated, where the addressed topic is highlighted, so as collaborations with the country.

Considering the current paradigm and relevance of this theme, the present work integrates the capabilities that the Portuguese Navy possesses in this scope, analyzing them through the NATO DOTMLPI-I approach (Doctrine, Organization, Training, Material, Leadership, Personnel, Infrastructure and Interoperability).

Keywords: cyberdefence, cyberspace, cybersecurity, National Strategy of Cyberspace Security, Portuguese Navy.

Índice

Lista de Abreviaturas, Siglas e Acrónimos

ADU - Administrador do Domínio do Utilizador

AESD - Agência Europeia de Segurança e Defesa

ANC - Autoridade Nacional de Cibersegurança

ANC - ANS - Autoridade Nacional de Segurança

C4ISR - Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CCD - Centro de Ciberdefesa

CCD COE - Cooperative Cyber Defence Centre of Excellence

CDMA - Cyber Defence Management Authority

CEDN - Conceito Estratégico de Defesa Nacional

CEMA - Chefe do Estado-Maior da Armada

CEMGFA - Chefe do Estado-Maior-General das Forças Armadas

CERT - Computer Emergency Response Team

CFP - Curso de Formação de Praças

CFS - Curso de Formação de Sargentos

CIISS - Cyber Information and Incident Coordination System

CIRC - Computer Incident Response Capability

CIS - Comunicações e Sistemas de Informação

CMX - Crisis Management Exercise

CNCS - Centro Nacional de Cibersegurança

COMNAV - Comando Naval

COMPUSEC - Segurança dos Computadores

COMSEC - Segurança das Comunicações

CPOCIBER - Curso de Planeamento de Operações De Ciberdefesa

CRISI - Capacidade de Resposta a Incidentes de Segurança da Informação

CRYPTO – Segurança da Criptografia

CSIRT - Computer Security Incident Response Team

CSSC - Conselho Superior de Segurança do Ciberespaço

DDoS - Distributed Denial of Service

DIRCSI - Direção de Comunicações e Sistemas de Informação

DITIC - Direção de Tecnologias de Informação e Comunicações

DL -Decreto-Lei

DJOI - Departamento Jurídico Operacional e Internacional

DOTMLPI-I - Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade

DR – Decreto Regulamentar

EC3 – European Cybercrime Centre

EDA - European Defense Agency

EMA – Estado-Maior da Armada

EMGFA - Estado-Maior General das Forças Armadas

EMSEC – Segurança das Emissões

EN - Escola Naval

ENISA – European Network and Information Security Agency

ENSC - Estratégia Nacional de Segurança do Ciberespaço

ENSI - Estratégia Nacional de Segurança da Informação

ETNA - Escola de Tecnologias Navais

EUA - Estados Unidos da América

EUROPOL - European Police Office

ExNCS - Exercício Nacional de Cibersegurança

FFAA - Forças Armadas

FOC - Full Operational Capability

GNS - Gabinete Nacional de Segurança

GODU - Gestor Operacional do Domínio do Utilizador

GPNS - Gabinete de Projetos, Normalização e Segurança

GSI - Gabinete de Sistemas de Informação

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

GT-EMA - Grupo de Trabalho do Estado-Maior da Armada

IDN – Instituto da Defesa Nacional

INFOSEC - Segurança da Informação

ISO - International Organization for Standardization

IUM - Instituto Universitário Militar

J-CAT - Joint Cybercrime Action Taskforce

LOBOFA - Lei Orgânica de Bases da Organização das Forças Armadas

MDN – Ministério da Defesa Nacional

MISP - Malware Information Sharing Platform

MN CD E&T - Multinational Cyber Defence Education and Training

NAC - North Atlantic Council

NATO - North Atlantic Treaty Organization

NCIA - NATO Communications and Information Agency

NCIA - NATO Communications and Information Academy

NCIRC - NATO Computer Incident Response Capability

NCIRC – Núcleo Computer Incident Response Capability

NSWAN - NATO Secret Wide Area Network

OCAD - Órgão Central de Administração e Direção

OSDU - Oficial de Segurança do Domínio do Utilizador

PAFM - Plano de Anual de Formação de Marinha

PCA – Publicação de Comunicações da Armada

PCSD - Política Comum de Segurança e Defesa

PJ - Polícia Judiciária

RCM – Resolução do Conselho de Ministros

SI - Sistemas de Informação

SIC - Sistemas de Informação e Comunicação

SICA - Sistemas de Informação e Comunicação Automatizados

SIS - Serviço de Informações de Segurança

SRI - Segurança das Redes e da Informação

STI - Superintendência das Tecnologias da Informação

TI - Tecnologias da Informação

TIC - Tecnologias da Informação e Comunicação

TRANSEC - Segurança das Transmissões

UE - União Europeia

UEO - Unidades, Estabelecimentos e Órgãos

Índice de Figuras

Introdução

Enquadramento do Tema

Com a globalização e a revolução tecnológica, conceitos caracterizadores do século XXI, surgiu uma nova dinâmica nos processos de interação. O uso generalizado da Internet[1] e das tecnologias da informação e comunicação (TIC) permitiram uma transformação social, cultural, política e económica, numa sociedade reconhecida como a Sociedade da Informação[2], definida pela partilha e pelo rápido e fácil acesso à informação, onde "a geração, processamento e transmissão de informação torna-se a principal fonte de produtividade e poder" (Castells, 1999).

A Internet converteu-se num instrumento imprescindível para o desenvolvimento e prosperidade das sociedades. Com a crescente dependência dos Estados, organizações e cidadãos na utilização do ciberespaço, foram potencializadas as suas capacidades e simultaneamente, cresceram os riscos e as ameaças associados ao seu uso potencialmente devastador.

O ciberespaço pode ser assumido como um espaço construído "pelo conjunto de sistemas informáticos, redes de comunicação e informação neles processada e armazenada" (Santos, 2012), "onde virtualmente todos os sistemas têm o potencial de comunicar entre si" (Neves, 2015). O qual constitui a base de muitas das infraestruturas nacionais, algumas das quais críticas e onde assentam muitos dos serviços essenciais, como as redes de transportes, de energia e de telecomunicações.

A interligação criada pela rede digital e respetivas máquinas associadas, caracterizada pela ausência de limites físicos ou territoriais, denominada por Manuel Castells de Sociedade em rede, oferece uma realidade onde se equacionam novas questões de segurança que exigem o contributo dos seus vários operadores, desde o público ao privado, até ao utilizador em casa (Castells, 2007). Num discurso proferido pelo Eng.º

[1] Segundo o PDA 2, que remete para o Glossário de Terminologia Informática, da CT 113, a Internet é uma "imensa rede de redes que se estende por todo o planeta e praticamente por todos os países; os meios de ligação dos computadores desta rede são variados, compreendendo linhas telefónicas tradicionais, linhas digitais, fibras óticas, comunicação por satélite, etc." (EMA, 2006).

[2] Conceito desenvolvido inicialmente por Peter Drucker, em 1966, no seu livro *The Age of Discontinuity*, onde menciona que a o poder da economia da sociedade evoluiu da agricultura para a indústria, desta última para os serviços e, por fim, para a informação (Crawford, 1983).

António Guterres, secretário-geral das Nações Unidas, em fevereiro de 2018, é destacada a cibersegurança como método que deve acompanhar sempre o manuseio das TIC.

O uso massivo das TIC conduz ao aparecimento e constante evolução de um leque variado de ameaças cibernéticas, das quais o ciberterrorismo e a cibercriminalidade são identificadas, na Orientação Política para a Ciberdefesa, como ameaças e riscos prioritários, capazes de "provocar o colapso da estrutura tecnológica da organização social e económica do País" (Despacho n.º 13692/2013 de 28 de outubro).

Neste sentido, foi proposto recentemente, pelo grupo parlamentar do Partido Socialista (PS), o projeto de lei n.º 1217/XIII, denominado de *Carta de Direitos Fundamentais na Era Digital*. O documento realça a crescente relevância do presente tema para um desenvolvimento sustentável global, alertando simultaneamente para as consequências da evolução digital (PS, 2019).

O projeto de lei sugere que "as normas que na ordem jurídica portuguesa delimitam e protegem direitos, liberdades e garantias" sejam "plenamente aplicáveis ao ciberespaço" (PS, 2019), evidenciando no âmbito nacional, uma maior atenção e empenho empregues às questões cibernéticas.

Pelo enorme impacto que o uso incorreto ou malicioso do ciberespaço pode ter em todos os setores da nossa sociedade, o papel a desempenhar pelo Estado na delineação de uma estratégia e políticas neste âmbito torna-se fundamental. Cabe a cada governo tomar medidas adequadas para garantir um ciberespaço livre e seguro, capaz de reduzir ou amenizar as vulnerabilidades inerentes à sua crescente evolução e utilização.

Por esta razão e, mais especificamente no âmbito desta dissertação, é crucial que a Marinha Portuguesa incorporada nas Forças Armadas (FFAA) de Portugal, promova a segurança do seu ciberespaço de interesse.

Justificação do Tema

Com toda a problemática envolta na segurança das várias redes e dos serviços associados a elas, questiona-se inclusive a Segurança Nacional[3] e a soberania[4] do Estado.

[3] Segurança Nacional é "a condição que visa a obtenção e a manutenção dos objetivos e interesses da Nação, por meio da integração e do emprego coordenado das várias expressões do Poder Nacional", apresentado em artigo da Revista Militar, com referência para o General Silveira apresentado pelo Exército Brasileiro, em 2002 (Cunha, 2018).

[4] O conceito de soberania do Estado Português consta da Constituição da República Portuguesa nos artigos. 1.º, 2.º, 3.º e manifesta-se na ordem internacional e nas relações externas entre estados, que pelo Manual de Tallinn entende-se como a "independência em relação a uma parte do globo [sendo] o direito

Face a este novo paradigma, Portugal e as organizações das quais faz parte, definiram e adotaram doutrina num esforço de prevenir e combater os riscos e ameaças cibernéticos.

No teor deste estudo, compete às FFAA garantir a Defesa Nacional. Não sendo um conceito isolado da Segurança Nacional, tem como objetivo "garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas" (Assembleia Constituinte, 1976).

O atual paradigma da Marinha, muito dependente a nível tecnológico, apresenta especial destaque para a sua capacidade de comando e controlo e para o apoio à decisão (EMA, 2012). As interligações de rede estabelecidas com as restantes FFAA, a Defesa Nacional, a *North Atlantic Treaty Organization* (NATO), a União Europeia (UE) e a sociedade civil, revelam-se mais um fator de vulnerabilidade através do comprometimento entre as várias interligações existentes.

Tomando esta realidade em consideração, o atual Chefe do Estado-Maior-General das Forças Armadas (CEMGFA) António Silva Ribeiro, assina a Diretiva Estratégica 2018-2021, com a missão de "garantir a defesa militar da República, contribuir para a segurança nacional e internacional e apoiar o desenvolvimento e o bem-estar das populações". Neste documento, é inserido no quadro das vulnerabilidades, a "deficiente capacidade para fazer face aos desafios do mundo digital" transpondo para um dos seus objetivos estratégicos a "edificação da capacidade de ciberdefesa nacional" (*Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2018-2021*, 2018).

Igualmente com a mesma preocupação, o Chefe do Estado-Maior da Armada (CEMA) subscreve a Diretiva Estratégica da Marinha 2018, com a visão de uma Marinha "ao serviço de Portugal e da segurança coletiva" para a missão de "contribuir para que Portugal use o Mar" (*Diretiva Estratégica da Marinha 2018*, 2018), onde são mencionadas as ciberameaças nos quadros da vulnerabilidade e das ameaças externas.

A Marinha estabelece por este motivo, uma linha estratégica com o intuito de reforçar a sua capacidade de ciberdefesa nacional, envolvendo a qualificação dos operadores, a execução de métodos e meios para proteger a informação e os sistemas, e a

---

de exercer o mesmo, com exclusão de qualquer outro Estado, as funções de um Estado" (tradução da autora).

consciencialização dos vários utilizadores das redes e respetivos sistemas de informação e comunicação (SIC).

Neste sentido, em virtude da pertinência que este tema tem na atualidade e para as funções que a Marinha Portuguesa se compromete a exercer, considera-se relevante e necessário enquadrar juridicamente e analisar as capacidades que a Marinha tem neste âmbito, reconhecendo as suas fragilidades e alguns dos contributos que poderão ser úteis para a segurança do seu ciberespaço de interesse.

Objetivos

O principal objetivo desta dissertação é percecionar a capacidade de cibersegurança da Marinha Portuguesa e, por consequência, alertar este ramo militar para a necessidade de reconhecimento das questões a abordar nesta matéria.

Para tal, foram definidos os subsequentes objetivos:

- Compreender a evolução do conceito do ciberespaço e questões associadas;
- Reconhecer a importância da implementação de medidas de segurança do ciberespaço;
- Compreender a articulação entre os conceitos de cibersegurança e ciberdefesa;
- Enquadrar a política de cibersegurança a nível da NATO e da UE, relativamente a Portugal;
- Enquadrar as medidas adotadas e implementadas por Portugal neste âmbito;
- Analisar a doutrina existente e aplicável às FFAA, nomeadamente, à Marinha;
- Verificar como são coordenados os esforços entre as várias entidades com responsabilidade em Portugal e na Marinha, caso ocorram ciberincidentes ou ciberataques;
- Averiguar nas estruturas e orgânica da Marinha com responsabilidades na monitorização e implementação de medidas de cibersegurança, quais as suas funções e como as executam;
- Verificar como os restantes Unidades, Estabelecimentos e Órgãos (UEO) respondem aos procedimentos e cuidados a ter para a segurança do ciberespaço;
- Identificar as deficiências e as fragilidades que a Marinha detém nesta área.

Metodologia de Investigação

Para a realização da presente dissertação, foi utilizada a metodologia de investigação baseada no método de Quivy e Campenhoudt para as ciências sociais e humanas. Conforme o sugerido por esta metodologia, formulou-se a questão principal "Que capacidade a Marinha Portuguesa tem no âmbito da cibersegurança?" e as suas questões derivadas:

- Que legislação precede a capacidade de cibersegurança da Marinha?
- De que forma é efetuada a prevenção, monitorização e resposta aos incidentes ocorridos no ciberespaço de interesse da Marinha?
- Como se articula e é aplicada a legislação existente com o desenvolvimento da capacidade de cibersegurança da Marinha?

Com o objetivo de responder às questões de partida, realizou-se a pesquisa de informação e a sua análise. Após um enquadramento teórico do tema abordado, foram analisadas as diferentes vertentes que compõem uma capacidade operacional e concorrem para a gestão e desenvolvimento da segurança do ciberespaço da Marinha, realizando neste âmbito diversas entrevistas a entidades com funções ao nível da cibersegurança e ciberdefesa nacional. Por fim, terminou-se o presente trabalho com uma análise crítica numa síntese conclusiva.

Estrutura do Documento

A presente dissertação encontra-se estruturada da seguinte forma:

Na introdução, é apresentado um breve enquadramento relativamente à evolução tecnológica e respetivo impacto, justificando a pertinência do tema abordado, os seus objetivos e a metodologia seguida.

No capítulo 1, são introduzidas as definições dos conceitos fundamentais para o desenvolvimento deste trabalho.

No capítulo 2, aborda-se a organização para a cibersegurança e ciberdefesa nas componentes legal, estratégica, operacional e técnica, na NATO, na UE e em Portugal, contextualizando o tema da dissertação num âmbito nacional e internacional.

No capítulo 3, é analisada a capacidade de cibersegurança da Marinha segundo a abordagem DOTMLPI-I[5] da NATO, enquadrando-a juridicamente com a Estratégia Nacional da Segurança do Ciberespaço (ENSC) e a Lei n.º 46/2018, de 13 de agosto, entre outros documentos doutrinários. No desenvolvimento deste capítulo, insere-se ainda a análise das entrevistas realizadas.

Por fim, na conclusão apresenta-se a síntese do trabalho desenvolvido, tendo como base os objetivos inicialmente propostos, e são sugeridos trabalhos futuros.

[5] Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade. Esta metodologia foi definida pela NATO como o conjunto dos domínios que permitem edificar uma capacidade operaciona.

1. Enquadramento Teórico

1.1. Ciberespaço: Conceito e Caracterização

Na esfera deste tema, torna-se pertinente e útil clarificar os conceitos indispensáveis à construção desta dissertação e referentes ao *cyber stuff*[6], de forma a compreender no que consiste e o motivo da sua crescente importância nas novas políticas e estratégias nacionais e internacionais. Dos neologismos resultantes do prefixo ciber, realça-se o termo ciberespaço, que foi originalmente cunhado por William Gibson, na sua obra *Neuromancer*, em 1984, e ao qual se refere como um universo abstrato da informação, utilizado por bilhões de cidadãos diariamente.

Castells explica a expansão e o destaque do ciberespaço cronologicamente. Escreve que apesar da internet ter crescido na mente dos cientistas da computação no início de 1960 e ter-se desenvolvido no seio desta comunidade na década seguinte, só em 1995 é que realmente nasceu para a restante sociedade (Castells, 2003).

Gibson concedeu originalmente, uma definição vaga ao ciberespaço, contudo, este conceito foi-se complementando com explicações análogas de vários autores ao longo dos anos, sem entretanto se ter atribuído uma definição comum a este termo. Assim, o filósofo francês Pierre Lévy, menciona o ciberespaço como:

> "O novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo" (Lévy, 1999).

Esta definição, é reiterada pela *International Organization for Standardization* (ISO), em 2012, como "o ambiente complexo resultante da interação de pessoas, softwares e serviços na Internet por meio de dispositivos de tecnologia e redes conectadas a ele, que não existe em nenhuma forma física" (CCDCOE, n.d.-b).

[6] Expressão referida por um *senior leader* do US *Departement of Defense* numa conferência em Washington DC (Singer & Friedman, 2014).

Já a NATO, em 2014, atribuiu uma outra definição ao ciberespaço, afirmando que consiste no "ambiente global que é criado através da interconexão de sistemas de comunicação e informação", excluindo a componente humana e enfatizando apenas "as redes de computadores físicas e virtuais, sistemas de computadores, *digital media* e dados" (NATO, 2014a).

Entre as diversas explicações empregues ao mesmo conceito, pode-se dizer que a sua maioria se refere a este termo como um espaço virtual composto por um conjunto de contribuintes, físicos (i.e. máquinas) e não físicos (i.e. informação), que de forma interligada, têm a capacidade de comunicar entre si e permitir assim, a sua existência.

Nesta dissertação, serão adotadas as definições dadas por Lévy e pela ISO, que por diferentes palavras referem o mesmo. As componentes materiais e virtuais centram-se na parte técnica desta dissertação e as componentes organizacional e operacional inserem-se no enquadramento jurídico.

Este novo paradigma, tornou possível um abrupto crescimento económico em empresas, organizações e nações, com a descentralização de empresas e organizações e a independência temporal e espacial vivida na comunicação entre os vários utilizadores do ciberespaço, que se podiam inclusive encontrar em qualquer parte do planeta. Tendo consciência dos benefícios associados à utilização do ciberespaço, assistiu-se à sua enorme aderência e dependência por parte dos Estados, das empresas e até mesmo dos cidadãos.

Neste novo domínio, Barry Posen, professor de Ciência Política no MIT, caracteriza o ciberespaço como um *global common*, definindo estes espaços como os "espaços que não estão sob o controlo direto de qualquer Estado mas que são vitais para o acesso e ligação a quaisquer pontos do mundo" e que inclui as águas internacionais, o espaço aéreo internacional e o espaço exterior (Viana, 2012).

Contudo, Joseph Nye, professor emérito na *Kennedy School of Government* da Universidade Harvard, refuta que o ciberespaço possa ser considerado como um *global common*, referindo que alguns dos seus constituintes podem ser controlados pelo próprio Estado. O exemplo mais notável disso é o sistema de censura da China, intitulado de Escudo Dourado[7].

[7] Desde 2003, o governo chinês instaurou um sistema de censura que permite vigiar e controlar os conteúdos acedidos online pelos seus cidadãos.

Pode-se afirmar então, em referência aos estados de direito democráticos e de um modo geral, que o ciberespaço se caracteriza como um espaço acessível e de comunicação livre. A inexistência de fronteiras no ciberespaço e a impossibilidade de definir limitações tecnológicas pelos Estados, que simultaneamente têm o dever de respeitar os direitos e liberdades dos cidadãos nos estados de direito democráticos, evidencia as diferentes abordagens de prevenção e de manutenção da segurança no ciberespaço.

Neste âmbito, as estratégias definidas pelos Estados deverão ter em conta uma harmonia entre o "crescimento económico-social advindo da utilização da Internet enquanto meio de livre circulação de informação e as necessidades de segurança do Estado e dos cidadãos" (Geraldes, 2013).

A rápida evolução tecnológica conjugada com a possível anonimidade do utilizador permite constatar a utilização do ciberespaço para fins maliciosos, incluindo ataques cibernéticos com impacto em larga escala de caráter transfronteiriço.

De acordo com o *Special Eurobarometer 464a – Europeans' attitudes towards cyber security*, em 2017, 42% dos utilizadores da Internet na UE afirmaram ter sido vítimas de *malware*[8] nos seus dispositivos, contra 47% dos utilizadores, em 2014. Embora com uma ligeira melhoria neste último parâmetro, possível indicador de uma melhor segurança no uso da Internet, o mesmo estudo indica que a ligeira maioria de 51% (face a 46%), considera estar mal informado quanto aos riscos do cibercrime, não apresentando uma diferença significativa em relação a 2014.

Por cibercrime pode entender-se como definição aplicável os "atos que violam tratados internacionais e leis nacionais, visando redes ou sistemas de informação, ou usando-os para cometer uma ofensa ou crime" (Agence Nationale de la Sécurité des Systèmes d'Information, 2011). No ordenamento jurídico português, aos designados cibercrimes, aplica-se a Lei n.º 109/2009, de 15 de setembro, e o Código Penal Português. Os cibercrimes representam uma fação das ciberameaças, termo que compreende igualmente o *hacktivismo*, a ciberespionagem, a ciberguerra, os ciberincidentes e o ciberterrorismo.

O conceito de ciberameaça, definido pela Finlândia, na sua Estratégia de Cibersegurança de 2013, representa "a possibilidade de ação ou de um incidente no domínio cibernético que, quando materializado, coloca em risco alguma operação

[8] *Malware* (*Malicious Software*) refere-se ao código ou ao programa cujo propósito é aceder sem autorização ou provocar danos num sistema informático, mostrando-se sob a forma de Vírus, *Worms*, cavalos de tróia, entre outros (Gelbstein, 2012).

dependente do mundo cibernético", especificando que estas ameaças são "ameaças de informação" e que "comprometem o correto ou pretendido funcionamento do sistema de informação" (CCDCOE, n.d.-b).

1.2. Ciberespaço enquanto domínio operacional

O comprometimento dos sistemas de informação, e inevitavelmente dos restantes sistemas e estruturas que a eles se interligam e que deles dependem, foi possível desde a criação e o desenvolvimento do ciberespaço.

Em 1971, Bob Thomas programou o primeiro vírus informático[9], denominado *The Creeper*, que correu no sistema da Arpanet[10]. Embora muito primitivo e sem o objetivo de danificar os sistemas, Thomas conseguiu provar que era possível introduzir programas numa rede informática, propagando-se de máquina em máquina, sem autorização do utilizador (Chen & Robert, 2004).

Na década de 1990, a Internet privatizou-se e desenvolveu-se como uma rede global[11] composta pela interligação de várias redes informáticas. Embora já se tivessem criado vários códigos maliciosos, a globalização da Internet permitiu que os mesmos tivessem uma maior capacidade de expansão e, somado aos exponenciais avanços tecnológico e informático, fossem capazes de causar danos mais significativos.

Em 1999, foi criado o *Melissa*, que se tornou até à data o vírus informático com maior poder de disseminação (Ramos, 2011). Este vírus enviava-se a si próprio através do *Outloook*, paralisando o funcionamento dos sistemas de correio eletrónico e criando uma reação em cadeia que infetou mais de um milhão de computadores em todo o mundo e provocou prejuízos de oito mil milhões de dólares.

Seguiram-se outros vírus com grande impacto, como o *I Love You*, em 2000, que se auto propagava pelos endereços de e-mail do utilizador assim que fosse aberto e que causou prejuízos acima dos cinco mil milhões de dólares. Em 2004, foi lançado o vírus

[9] Vírus informático é definido pelo Glossário Espanhol como um "programa desenhado para se copiar a si mesmo com a intenção de infetar outros programas ou ficheiros" (Centro Criptológico Nacional, 2015).
[10] A Arpanet (*Advanced Research Projects Agency Network*) foi a rede pioneira da Internet, que consistia numa rede de computadores criada pelo Departamento de Defesa dos EUA em 1969 e utilizada até 1990, com o objetivo de partilhar informações para fins militares.
[11] Tim Berners-Lee, um programador inglês, desenvolveu em 1990 a *World Wide Web* (www) que permitiu a globalização da Internet.

Sasser que inoperacionalizava os computadores através de uma vulnerabilidade do Microsoft Windows e infetou mais de um milhão de computadores, causando dezoito mil milhões de dólares em prejuízos.

Mais recentemente, surgiram os *ransomwares Petya*, em 2016, e *WannaCry*, em 2017, sendo que o primeiro ressurgiu com uma nova versão em 2017. Caracterizavam-se ambos pela restrição do acesso a todo o disco rígido ou aos ficheiros do computador, respetivamente (Avast, n.d.-a, n.d.-b). Em troca exigiam o pagamento de uma determinada quantia, para o utilizador poder ter acesso ao que havia sido restrito. Ambos os *ransomwares* originaram impacto a nível mundial, em empresas, organizações, hospitais, aeroportos, entre outros.

Estes foram alguns dos vírus que tiveram um grande impacto na sociedade em geral, no entanto, a sua sofisticação e a crescente potencialidade das suas consequências, transformaram o ciberespaço num terreno apto a provocar ataques dirigidos a nações alvo. Esta capacidade traduz-se no conceito de ciberguerra, que se traduz no "uso de computadores para interromper as atividades de um país inimigo, especialmente o ataque deliberado de sistemas de comunicação" (Maurer, T., & Morgus, 2014).

Remetendo ao ano de 1999, a NATO foi alvo das primeiras ameaças cibernéticas aquando a campanha aérea no Kosovo (Monteiro, 2016). O conflito existente entre a organização e a Sérvia, originou o ataque a infraestruturas de Internet por parte de *crackers*[12] pró-sérvios. Como resultado, vários sistemas de informação e comunicação da NATO, tal como os de alguns países aliados foram comprometidos (Geers, 2008).

Em 2007, a Estónia, um país muito avançado tecnologicamente e onde a maioria dos seus serviços essenciais são utilizados online pelos seus cidadãos, viu-se paralisada durantes semanas devido a uma vaga de ciberataques sofridos sob a forma de *Distributed Denial of Service* (DDoS) [13] (Ramos, 2013).

Esta sucessão de eventos ficou reconhecida como a primeira ciberguerra da história, alegadamente perpetuada por *crackers* russos[14] e provocou o cancelamento ou incorreto

[12] Termo utilizado para designar peritos informáticos que acedem a sistemas informáticos sem autorização. Surgiu do termo *hacker*, que representa igualmente peritos informáticos mas que de forma legal exercem as suas funções.
[13] DDoS é um ataque feito a um alvo, como um servidor ou um *website*, através de vários sistemas de computadores comprometidos e que resulta na negação de serviços para os utilizadores do recurso de destino (Rouse, 2019).
[14] A autoria deste ataque trata-se de informação sem confirmação oficial quanto à fonte do incidente, tal como o ataque proferido à Geórgia.

funcionamento de muitos dos seus serviços virtuais, tais como de bancos, escolas e jornais (Clarke & Knake, 2012).

No ano seguinte, foi a vez da Geórgia ser vítima de ciberataques supostamente também por cidadãos russos, aquando a sua invasão pela Rússia. Estes ataques, similares aos provocados à Estónia, resultaram na negação de *websites* governamentais, entre outros serviços. Segundo a NATO, este conflito revelou que os "ataques cibernéticos têm o potencial de se tornar um componente importante da guerra convencional" (NATO, 2018e).

Em 2010, foi denunciado um ataque cibernético direcionado a um serviço específico de um país, o Irão. O *Stuxnet* foi um vírus informático que atacava especificamente um software industrial, comprometendo algumas das centrais que produziam material nuclear e que resultou num atraso de vários anos no programa nuclear iraniano (Theiler, 2011).

Estes últimos casos constituem exemplos da utilização do ciberespaço como um novo espaço de guerra e um alerta para os Estados da potencial destruição ou danificação que ataques cibernéticos podem causar à nação, fazendo ver que os mesmos devem assegurar aos seus cidadãos uma utilização segura do ciberespaço e salvaguardar a própria soberania (Freire & Nunes, 2013).

Neste sentido, na Cimeira de Varsóvia, em 2016, a NATO assumiu o ciberespaço como um novo domínio operacional, tal como o ar, a terra e o mar, com o intuito de melhorar as capacidades de proteção e condução de operações neste novo domínio (NATO, 2016c). Podendo-se afirmar que no atual paradigma digital, "qualquer pessoa com um computador e uma conexão à Internet é um potencial combatente" (Geers, 2008).

Pelos exemplos constados acima, é sustentada a responsabilidade de cada Estado em "equacionar e considerar (…) o levantamento de capacidades militares neste domínio, sob pena de não conseguir assegurar a defesa dos seus interesses e o exercício da sua própria soberania" (Nunes, 2018).

Deste modo, muitos países reconheceram a importância do ciberespaço não só como criador de novas oportunidades, como também de novos riscos e ameaças, resultando na edificação, desenvolvimento e implementação de estratégias nacionais, por forma a garantir a segurança e a defesa do ciberespaço (Carvalho, 2017).

1.3. Cibersegurança e Ciberdefesa

Para a segurança e defesa do ciberespaço, formam-se dois conceitos distintos, mas onde as fronteiras são algo ténues: a cibersegurança e a ciberdefesa. Independentemente da finalidade de ambas as vertentes, estas pretendem manter os requisitos que garantem a qualidade da informação.

Deste modo, os princípios básicos que garantem a segurança da informação consistem na confidencialidade, a propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas ou segundo processos não autorizados; na integridade, a propriedade de salvaguardar o carácter exato e completo dos ativos e da informação; e na disponibilidade, a propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada. Devem ainda ser consideradas a autenticidade, a garantia de que a informação é genuína e provém de fonte fidedigna; e o não repúdio, a capacidade de provar que um ato ou acontecimento teve lugar, de modo a que esse acontecimento ou ato não possa ser subsequentemente negado (Decisão (UE, Euratom) 2015/444 de 13 de março; Andress, 2014; Despacho n.º 13692/2013 de 28 de outubro).

Paralelamente, a segurança ao nível dos SIC distingue-se em três áreas, a segurança física das instalações e o controlo das mesmas, a segurança em função do pessoal que tem acesso a informação classificada e a segurança do material em contacto com a informação (Neves, 2015), tal como referido na figura seguinte.

Figura 1 Esquemático da segurança dos Sistemas de Informação e Comunicações

Fonte: Neves, 2015

Como exposto na figura 1, a cibersegurança originou-se da articulação entre a segurança da informação (INFOSEC) e as Operações em Redes de Computadores, a nível da Exploração e da Defesa. Mais especificamente, a INFOSEC traduz-se nas medidas implementadas para garantir a segurança da informação (Andress, 2014) e divide-se em outras duas áreas, a segurança das comunicações (COMSEC) e a segurança dos computadores (COMPUSEC). Por sua vez, a COMSEC reparte-se na segurança das Transmissões (TRANSEC), das Emissões (EMSEC) e da Criptografia (CRYPTO) e o COMPUSEC resume-se na segurança do *hardware*, do *software* e do *firmware*[15] dos computadores (DITIC-NCIRC, 2018; Neves, 2015).

Relativamente às Operações em Redes de Computadores, estas divergem na Exploração das atividades e operações que ocorrem no ciberespaço com o propósito de as conhecer e as entender, na Defesa das Redes para proteção dos SIC contra possíveis ataques e vulnerabilidades existentes e, por fim, no Ataque que possibilita às forças militares "a disrupção, a negação, a degradação ou mesmo a destruição dos sistemas de informação do inimigo" em caso de necessidade (DITIC-NCIRC, 2018; Neves, 2015). O conjunto das Operações em Rede agregado à COMPUSEC originou o termo ciberdefesa.

Segundo Paulo Moniz, no seu sentido lato, pode-se entender a cibersegurança como o "conjunto das atividades, que ocorrem no ciberespaço, de prevenção, monitorização e resposta às ameaças que, pela sua natureza disruptiva, coloquem em risco o bem-estar e a salvaguarda dos direitos dos cidadãos ou organizações" e a ciberdefesa como "as atividades de prevenção, monitorização e reação a ameaças que coloquem em risco a soberania nacional, sendo que compete às Forças Armadas assegurar a missão da ciberdefesa" (Moniz, 2018).

Numa outra perspetiva, Pedro Veiga, coordenador do Centro Nacional de Cibersegurança (CNCS) de abril de 2016 a maio de 2018, refere-se à cibersegurança como um "conjunto de medidas técnicas, organizativas e de capacitação das pessoas destinadas à proteção das redes, dos sistemas de informação e dos dados", mais especificamente ao mundo civil, e à ciberdefesa como a área que "trata da cibersegurança para o ambiente estrito militar, mas compreende também outas vertentes como sejam o desenvolvimento de capacidades ofensivas no ciberespaço" (Veiga, 2018).

[15] *Hardware* são os componentes físicos que constituem o sistema operativo de um computador ou de outro dispositivo de telecomunicações, *software* são as instruções que podem ser armazenadas e executadas pelo *hardware*. *Firmware* é similar ao *software* e consiste em instruções para controlar o hardware e colocadas na sua fabricação (GlossaryTech, n.d.; Techopedia, n.d.).

Segundo a Estratégia da União Europeia para a Cibersegurança, o conceito da cibersegurança é atribuído "às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrente da interdependência da suas redes e infraestruturas informáticas ou que as possam danificar" (JOIN(2013) 1 final).

Para esta dissertação, será empregue o conceito de cibersegurança como parte integrante da ciberdefesa e com as características apresentadas no parágrafo anterior. Ainda decorrente da mesma fonte, a cibersegurança visa "manter a disponibilidade e a integridade das redes e infraestruturas informáticas ou que as possam danificar" (JOIN(2013) 1 final). São as suas capacidades técnicas que passam pela prevenção, deteção e recuperação dos SIC perante ciberataques que relacionam estes dois conceitos, previstos na Orientação Política para a Ciberdefesa (Despacho 13692/2013 de 28 de outubro).

Com base nas definições apresentadas anteriormente e tendo em conta o presente estudo ser realizado a respeito de um ramo das FFAA, estes conceitos estarão constantemente relacionados, pois pretende-se que a Marinha enquanto organização preserve o seu bem-estar e a salvaguarda dos seus direitos, contribuindo igualmente para a cibersegurança nacional, e enquanto ramo militar, assegure a soberania nacional. Em termos de Operações em Rede, será unicamente desenvolvido e analisado as Operações de Defesa, excluindo a vertente da Exploração e do Ataque

2. Organização para a Segurança e Defesa do Ciberespaço

A segurança do ciberespaço tornou-se um ponto crítico e, consequentemente, uma prioridade nas estratégias e políticas das nações tendo em conta o grande impacto que pode ter no quotidiano da sociedade e na soberania do próprio país. Foi desta forma, que várias nações e organizações estabeleceram e implementaram na sua organização, medidas para a garantia da segurança e da defesa do ciberespaço. Neste sentido, ao longo do presente capítulo será abordada esta temática, tanto nas principais organizações das quais Portugal faz parte, bem como a nível nacional.

2.1. North Atlantic Treaty Organisation

A NATO, criada em 1949, representa uma organização constituída atualmente por 29 países, dos quais Portugal faz parte desde o ano do seu estabelecimento, e cuja missão é "garantir a liberdade e segurança dos seus membros através de meios políticos e militares" (NATO, n.d.).

Esta organização teve sempre como preocupação a proteção dos seus sistemas de comunicação e informação, contudo foi após o ataque proferido às redes e sistemas da NATO, durante a campanha aérea no Kosovo, em 1999, que a alertou para esta questão.

Como resultado, em 2002, com a Cimeira de Praga, a NATO inseriu pela primeira vez a ciberdefesa na sua agenda política com o objetivo de se adaptar aos novos desafios de segurança e fortalecer as suas capacidades de defesa face a ataques cibernéticos (NATO, 2002).

Desta cimeira resultou a criação do NATO *Computer Incident Response Capability* (NCIRC) que permite à NATO "prevenir, detetar, responder e recuperar de incidentes de cibersegurança" (NCIA, n.d.-c), apoiando também as capacidades de ciberdefesa dos aliados.

Em 2006, na Cimeira de Riga, a Aliança reforça a necessidade de proteger os seus sistemas de informação a longo prazo e de desenvolver o programa "NATO *Network Enabled Capability* para partilhar informação, dados e *intelligence* de forma confiável, segura e sem atrasos nas operações da Aliança" (NATO, 2006).

No ano de 2007, a onda de ciberataques maciços à Estónia demonstrou a potencial vulnerabilidade dos países aliados e até da própria NATO em relação aos seus SIC, revelando que os países "extremamente dependentes das comunicações eletrónicas, também eram extremamente vulneráveis na frente cibernética" (Theiler, 2011). Neste sentido, a NATO considerou ser de caráter urgente a melhoria da capacidade de proteção dos sistemas de informação críticos (NATO, 2007) e em 2008, na Cimeira de Bucareste, aprova a sua primeira Política de Ciberdefesa.

Com o objetivo de prevenir e responder a ciberataques, a Política de Ciberdefesa assenta nos pilares de subsidiariedade, auxiliando os aliados só no caso de pedirem assistência, caso contrário será da responsabilidade dos Estados garantirem a segurança e defesa dos seus SIC; de não duplicação, evitando a repetição desnecessária de estruturas e capacidades nesta área; e, por fim, de segurança, garantindo a cooperação entre os aliados com base na confiança de modo a garantir a segurança da informação sensível e que é acedida e utilizada pelos aliados (Theiler, 2011).

Esta política estabelece os princípios básicos para a ciberdefesa e providencia orientações neste âmbito não só para órgãos civis e militares da NATO, como também para os países aliados individualmente (*Defending against cyber attacks*, n.d.).

Da Política de Ciberdefesa 1.0 resultou a implementação, a nível estratégico, do *Cooperative Cyber Defence Centre of Excellence* (CCD COE) e a nível operacional, da *Cyber Defence Management Authority* (CDMA)(Hughes, 2009).

A CDMA, centralizada em Bruxelas, é responsável pela coordenação da ciberdefesa em toda a NATO e tem como objetivo melhorar a capacidade de defesa cibernética das nações NATO através de uma gestão em tempo real das ameaças cibernéticas.

O CCD COE, com sede em Tallinn, é "um centro de investigação e formação acreditado pela NATO que lida com a educação, consultadoria, lições aprendidas, pesquisa e desenvolvimento no campo da cibersegurança" (CCDCOE, n.d.-a), com a missão de melhorar a capacidade e a cooperação entre os países aliados e parceiros na ciberdefesa.

A ciberdefesa passou inclusivamente a integrar os exercícios da NATO. Organizado pelo CCD COE, desde 2008, é executado o exercício NATO *Cyber Coalition*, que visa treinar os procedimentos, a comunicação e a colaboração entre a NATO, os seus aliados e parceiros (NCIA, n.d.-b). Já desde 2010, surgiu o exercício *Baltic Cyber Shield*, que passou a ter mais tarde o nome de *Locked Shields* e atenta à defesa em tempo real de redes de computadores face a ataques cibernéticos (CCDCOE, 2017).

Em 2011, os ministros de defesa da NATO aprovaram a Política de Ciberdefesa 2.0 (NATO, 2012). Sobre a qual, Jamie Shea, atual secretário-geral da NATO para os Novos Desafios de Segurança desde 2010, comenta que:

> "Não só permitirá à OTAN defender as suas próprias redes de forma mais rápida e eficaz, como também prestar muito mais assistência aos Aliados e Parceiros em todas as três áreas cruciais da segurança cibernética: prevenção, lidar com os ciberataques e limitar o seu impacto e ajudar os países atacados a recuperar e restaurar rapidamente os seus sistemas de informações vitais" (Shea, 2011).

No ano seguinte, foi criada a NATO *Communications and Information Agency* (NCIA) que é responsável por obter, implementar e defender os sistemas de comunicação utilizados pela NATO (NCIA, n.d.-a). A NCIA passou a constituir-se como a linha da frente contra os ciberataques, cooperando com as nações aliadas e parceiros.

Em 2013, foi publicado o *Tallinn Manual on the International Law Applicable to Cyber Warfare*, produzido por um grupo internacional de especialistas independentes, a convite do NATO CCD COE em 2009. Esta proposta surgiu da necessidade em trazer algum esclarecimento às questões legais relativas às operações cibernéticas e representa a opinião de um grupo de especialistas, não servindo como um documento oficial ou doutrina NATO (Schmitt et al., 2013).

Em 2014, foi obtida a capacidade operacional total do NCIRC (NCIRC FOC (*Full Operational Capability*)), permitindo à NATO uma melhor proteção das suas redes. No mesmo ano, ocorreu a Cimeira de Gales, onde a NATO realçou uma vez mais a necessidade de defender eficazmente os seus SIC contra as ameaças cibernéticas que se vão tornando "mais comuns, sofisticadas e potencialmente prejudiciais" (NATO, 2014b).

A Aliança reconheceu que é da sua responsabilidade a proteção das suas próprias redes e apoia os seus estados membros, no entanto dita que é da responsabilidade de cada nação garantir a proteção das suas redes nacionais.

Do mesmo modo, a NATO reconheceu que o direito internacional é aplicado ao ciberespaço, pois os danos causados por um ciberataque podem ser tão prejudiciais quanto um ataque convencional. Neste sentido, o Estado que necessitar, após aprovação do *North Atlantic Council* (NAC), pode invocar o artigo 5.º do Tratado do Norte Atlântico:

> "As Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar,

> cada uma, no exercício do direito de legítima defesa, individual ou coletiva, reconhecido pelo artigo 51.° da Carta das Nações Unidas, prestará assistência à Parte ou Partes assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a ação que considerar necessária, inclusive o emprego da força armada, para restaurar e garantir a segurança na região do Atlântico Norte" (NATO, 1949).

A NATO assume assim a ciberdefesa como parte integrante da defesa coletiva. Na mesma declaração da Aliança, esta compromete-se a reforçar a cibersegurança das redes nacionais das nações aliadas, das quais também depende a sua segurança. Continuará a ser desenvolvida e melhorada a ciberdefesa nas operações da NATO, as parcerias e a cooperação com países, organizações e a indústria e, por fim, a educação, o treino e os exercícios nesta área (NATO, 2014b).

Em 2016, a NATO assume na Cimeira da Varsóvia, o ciberespaço como um domínio operacional, tal como o ar, a terra e o mar, com o objetivo de melhorar a proteção e a condução de operações neste novo espaço (NATO, 2016c). Esta nova assunção não altera a missão da NATO nesta área, que se mantém defensiva e de acordo com o direito internacional.

Foi também adotado pelos Chefes de Estado, o Compromisso de Ciberdefesa (*Cyber Defense Pledge*), onde os mesmos se comprometem a fortalecer as suas redes e infraestruturas nacionais de ciberdefesa, a fim de melhorar a sua resiliência e a capacidade de resposta às ciberameaças (NATO, 2016a).

No fim de 2016, a NATO e a UE estabeleceram um acordo para reforçar a sua cooperação para a segurança e defesa do ciberespaço através da participação em exercícios, da investigação, da formação de pessoal e da partilha de informação nesta área (NATO, 2016b). No ano seguinte, este acordo foi intensificado, realçando uma maior cooperação entre as duas organizações na adoção de boas práticas em matéria de cibersegurança e ciberdefesa e na gestão e resposta a incidentes cibernéticos (NATO, 2017a).

De acordo com a NATO, esta tem sido alvo de ciberataques com uma evolução crescente nos últimos anos e lida diariamente com atividade suspeita nas suas redes. Afirma ainda que em 2016, esta organização verificou cerca de 500 incidentes mensais, aproximadamente mais 60% do que 2015, e em 2017 ainda aumentou mais a estatística referente a ciberataques (NATO, 2018d).

Os Estados lidam com esta ameaça diariamente, com consequências para as sociedades modernas e para a Segurança Nacional a níveis cada vez mais preocupantes. Foi com isto em mente que, em 2017, foi publicada uma nova versão do Manual de Tallinn, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

Devido ao primeiro documento ter sido escrito com foco num contexto de conflitos armados, este novo surge com o objetivo de o expandir e o aplicar num contexto de tempo de paz, referente às atividades cibernéticas que ameaçam e afetam todos os dias os Estados (Schmitt et al., 2017). Nos mesmos moldes, este é um documento não oficial e expressa a opinião de vários peritos independentes em questões legais aplicadas a atividades cibernéticas.

Em 2018, na Cimeira de Bruxelas, a NATO acordou a criação de um Centro de Operações Ciber na Bélgica, a fim de "fornecer conhecimento situacional e coordenar as operações da NATO no ciberespaço" (NATO, 2018b). A Aliança considerou também a atribuição das capacidades de ciberdefesa nacionais nas missões e operações da NATO.

A NATO lançou, em maio de 2019, um recurso em linha denominado de *Cyber Law Toolkit*. Esta ferramenta permite, de uma forma interativa, o tratamento jurídico de questões relacionadas com a aplicabilidade do direito internacional a operações cibernéticas (UK ESRC IAA Project Co-Creation, 2019). O *Toolkit* foi criado com base em 13 cenários verídicos, abordando cada um deles através de uma análise jurídica.

Este projeto, a nível internacional, demonstra a relevância das questões cibernéticas e expetativas futuras na necessidade do seu tratamento a nível político jurídico e com possível impacto na soberania dos países envolvidos e exercício dos respetivos poderes inerentes, para efeitos de defesa ou de resolução de conflitos.

Sintetizando, ao longos dos últimos anos em que as questões cibernéticas começaram a entrar na agenda política da NATO, esta desenvolveu diversos esforços de modo a garantir e a melhorar a segurança e a defesa do ciberespaço.

A NATO assumiu a ciberdefesa como parte da sua defesa coletiva e como um novo domínio de operações, assumindo também a aplicabilidade do direito internacional no ciberespaço. Uma das suas prioridades passou por ser a proteção das suas redes e a melhoria das suas capacidades de resposta e recuperação a ciberataques e, individualmente, cada aliado comprometeu-se a melhorar as suas capacidades de ciberdefesa nacionais. Por fim, a NATO reforçou a sua cooperação com a UE e outros parceiros e o empenhamento na melhoria da formação, treino, exercícios e partilha de informação na área cibernética.

2.2. União Europeia

A União Europeia, constituída por 28 países e que acolheu Portugal em 1986, pretende promover a paz, a liberdade e a prosperidade dos seus estados membros. Esta união conta com a Comissão Europeia para propor "legislação, políticas e programas" de forma a cumprir com os seus objetivos e valores e com o Conselho Europeu para estabelecer "a orientação e as prioridades políticas gerais da UE" (Comissão Europeia, n.d.-b).

Em 2001, a Comissão adotou a Comunicação *Segurança das redes e da informação: Proposta de abordagem de uma política europeia*, onde assume a segurança das redes e da informação (SRI) como uma prioridade, tendo em conta o seu papel crucial e dependente na economia e na sociedade (COM(2001)298 final).

Com o objetivo de manter a disponibilidade, a integridade e a confidencialidade da informação e dos seus serviços agregados, face a eventuais acontecimentos ou ações maliciosas, propõe várias medidas. Nelas inserem-se a sensibilização para melhores práticas, o reforço das equipas de respostas a emergências informáticas (CERT - *Computer Emergency Response Team*) dos estados membros e uma melhor coordenação entre os mesmos, a criação de legislação para o cibercrime e uma melhoria na cooperação internacional referente a este domínio.

No mesmo ano, foi realizada uma Convenção de Budapeste sobre o Cibercrime, que se tornou o primeiro tratado internacional referente a cibercrimes e entrou em vigor na ordem jurídica internacional em 2004.

Este tratado prevê a criminalização dos comportamentos maliciosos e fraudulentos com definição no mesmo documento, a "criação de competências suficientes para combater eficazmente essas infrações" e a adoção de "medidas que visem uma cooperação internacional", em que cada estado membro deve dotar-se da sua própria legislação e meios para assegurar a segurança do seu ciberespaço (Council of Europe, 2001).

Em 2004, foi criada a Agência Europeia para a Cibersegurança (ENISA – *European Network and Information Security Agency*), em funcionamento desde 2005 e com a missão de "contribuir para um elevado nível de segurança das redes e da informação" da União e "desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, das empresas e das organizações" (Regulamento (CE) n.° 460/2004 de 10 de Março). A ENISA atua através de medidas de prevenção, deteção e resposta a

incidentes cibernéticos na UE, auxiliando também os seus estados membros quando necessário.

No mesmo ano, foi também criada a Agência Europeia de Defesa (EDA – *European Defense Agency*) que visa atualmente "aperfeiçoar as capacidades de defesa da União no domínio da gestão de crises e apoiar a Política Comum de Segurança e Defesa (PCSD) na sua atual configuração e na sua evolução futura" (DECISÃO (PESC) 2015/1835 de 12 de outubro). As suas prioridades compreendem a ciberdefesa através da cooperação com outras entidades da União, pela contribuição na investigação e desenvolvimento de tecnologia que apoiem esta área e pelo ensino e formação em matéria cibernética (European Defence Agency, 2015).

A partir de 2006, a UE adotou a *Estratégia para uma sociedade da informação segura*, com pretensão a reforçar e a modernizar a estratégia definida em 2001 pela Comissão, referente à segurança das redes e da informação. Esta estratégia estabelece medidas novas e complementares às anteriormente definidas para combater a cibercriminalidade (COM(2006) 251 final).

Em 2010, foi criado na Cimeira de Lisboa UE-EUA, de 20 de novembro, um grupo de trabalho com a parceira da UE e dos Estados Unidos da América (EUA) para a cibersegurança e a cibercriminalidade, que após reconhecer a importância das ameaças cibernéticas, comprometeu-se a desenvolver propostas nas várias vertentes críticas em matéria cibernética (União Europeia & United States, 2010), prestando desta forma apoio às políticas da UE.

Como parte da parceria UE-EUA, realizou-se em 2011, o exercício *Cyber Atlantic* por forma a identificar lacunas na cibersegurança e melhorar a colaboração entre os países envolventes no que toca à gestão de crises cibernéticas.

Neste âmbito, desde 2010, de dois em dois anos, ocorre o exercício de cibersegurança *Cyber Europe* gerido atualmente pela ENISA e onde participam os setores privado e público da União e dos países membros. Este exercício simula incidentes cibernéticos em grande escala e pretende treinar os participantes neste cenário, medindo o seu estado de preparação em cibersegurança e a eficácia da UE na gestão de cibercrises (ENISA, 2018a).

Em setembro de 2012, a UE instituiu permanentemente uma equipa de resposta a emergência informática. A CERT-UE é responsável por garantir a segurança dos sistemas informáticos dos órgãos da UE e cooperar com os CERT nacionais (ENISA, n.d.).

Em janeiro de 2013, o Centro Europeu de Cibercriminalidade (EC3 – *European Cybercrime Centre*) iniciou funções com a principal missão de combater o cibercrime na União Europeia, contando para isso com o trabalho conjunto de vários peritos nesta área que estudam e aplicam as vertentes legislativa e judicial (European Comission, 2019). O EC3 está integrado na agência *European Police Office* (EUROPOL) que visa o cumprimento da lei para garantir a segurança interna da UE e dos seus cidadãos.

O Centro atua através da criação de parcerias, medidas preventivas e de sensibilização nesta área, no desenvolvimento de normas políticas e legislativas que regulem estes crimes, no treino dos seus operacionais, na análise forense e num nível mais operacional, no combate a cibercrimes que resultem na extorsão de dinheiro, em graves consequências para pessoas, como a exploração sexual de menores, e por fim, que danifiquem infraestruturas críticas e sistemas de informação (EUROPOL, n.d.).

A esta última componente operacional, juntou-se em setembro de 2014, a *Joint Cybercrime Action Taskforce* (J-CAT) que representa uma autoridade internacional de combate ao cibercrime, inclusive fora da UE. O EC3 conta com a cooperação da agência europeia EUROJUST para apoiar judicialmente, por meio de ações penais, instrumentos jurídicos e partilha de informação, as autoridades competentes.

Em fevereiro de 2013, entra em vigor a *Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*. Em resposta às vulnerabilidades da UE, num tema em constante evolução e que ameaça a sociedade e a economia dos governos todos os dias, o referido documento pretende intensificar a cibersegurança na União e o seu desempenho a um nível geral, contando com a participação primeiramente de cada governo, bem como envolvendo outras parcerias (JOIN(2013) 1 final).

Esta estratégia tem patente que a legislação aplicada noutras áreas é empregue também no ciberespaço, que os direitos individuais e a liberdade de acesso à Internet e à informação devem ser preservados e que todos os utilizadores do ciberespaço, desde o Estado aos cidadãos individualmente, são responsáveis à sua medida por garantir um ciberespaço mais seguro.

Mais especificamente, a Estratégia define objetivos e medidas concretas a aplicar na prevenção, deteção e resposta aos ciberincidentes, estabelecendo cinco prioridades a cumprir: garantir a resiliência do ciberespaço; reduzir radicalmente a cibercriminalidade; desenvolver a política e as capacidades de ciberdefesa no quadro da PCSD; desenvolver os recursos industriais e tecnológicos para a cibersegurança; e, por fim, definir um política

internacional coerente sobre o ciberespaço para a UE, promovendo os seus valores fundamentais (JOIN(2013) 1 final).

Nas medidas impostas insere-se a obrigatoriedade dos governos adotarem, a nível nacional, uma autoridade competente neste domínio, um CERT operacional, uma estratégia e um plano de cooperação em matéria cibernética que permita a partilha de informação e uma ação coordenada entre as autoridades. Tendo em conta a participação do setor privado na gestão e no controlo das redes e dos sistemas de informação, o documento em questão visa também a criação de capacidades de cibersegurança por parte do mesmo setor. As medidas a aplicar contêm ainda a realização de mais exercícios para efeitos de treino da UE e a sensibilização dos cidadãos para manterem as redes e sistemas de informação seguros.

Em agosto de 2013, a União adotou a Diretiva 2013/40/UE para ataques contra os sistemas de informação e que pretende responsabilizar os infratores destes crimes pelos estados membros, através da aplicação do direito penal nesta matéria. Assim, o presente documento define regras mínimas para que os estados membros estabeleçam as suas medidas sancionatórias em função do crime cibernético cometido. Assume também que deve haver uma melhor cooperação entre as várias entidades nacionais e as pertencentes à UE encarregues de aplicar a lei nestes casos.

Em novembro de 2014, como resultado de uma das sugestões vinculadas na Estratégia da UE para a Cibersegurança e do reconhecimento do ciberespaço como um domínio operacional, é apresentado o *Quadro Estratégico da UE em matéria de Ciberdefesa* pelo Conselho, onde se destaca o apoio ao desenvolvimento de capacidades de ciberdefesa dos estados membros da UE, a melhoria de sinergias nas vertentes civil e militar e com o setor privado e a promoção da formação e do treino em ciberdefesa. Estes pontos estratégicos são assumidos no mesmo documento como prioritários e determinantes para o cumprimento da PCSD da UE (Conselho, 2014).

Em abril de 2016, o Parlamento Europeu e o Conselho da UE, publicam o Regulamento (UE) 2016/679, de 27 de abril, *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. O presente regulamento revoga a Diretiva 95/46/CE e passa a entrar em vigor em maio de 2018.

Em julho de 2016, a União admite que “as capacidades existentes não são suficientes para garantir um elevado nível de segurança das redes e dos sistemas de informação” devido à disparidade dos níveis de preparação dos seus membros (Diretiva (UE)

2016/1148 de 6 de julho). Do mesmo modo, constatou-se a carência de medidas comuns que abranjam os operadores de serviços essenciais e os prestadores de serviços digitais[16].

Assim, adotou-se a primeira legislação que estabelece requisitos mínimos em toda a UE para "cobrir todos os incidentes e todos os riscos relevantes" (Diretiva (UE) 2016/1148 de 6 de julho). Na Diretiva (UE) 2016/1148 *relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União* são definidas medidas e práticas de gestão de risco de cibersegurança que não devem ir contra as medidas estabelecidas por cada estado membro para a sua própria segurança.

A Diretiva SRI impõe aos estados membros que identifiquem o conjunto de operadores de serviços essenciais e os prestadores de serviços digitais nacionais para os mesmos tomarem as medidas necessárias de modo a prevenirem riscos de cibersegurança.

Simultaneamente, foi publicada a Comunicação para reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora. Esta comunicação propõe medidas para reforçar a resiliência da União Europeia em matéria de cibersegurança através de uma maior cooperação e intercâmbio de informações entre os órgãos da União, os estados membros e parcerias existentes (COM(2016) 410 final).

Neste seguimento, a Comissão apresenta a primeira parceria público-privada com a indústria sobre cibersegurança, sobre a qual Günter Oettinger, Comissário da Economia e Sociedade Digitais em 2016, comenta que

> "a Europa necessita de produtos e serviços de cibersegurança de elevada qualidade, interoperáveis e a preços acessíveis. [Tratando-se] de uma grande oportunidade para a indústria da cibersegurança competir num mercado mundial em rápido crescimento" (Comissão Europeia, 2016b).

O objetivo desta parceria é a colaboração entre as diferentes partes na investigação e desenvolvimento de soluções de cibersegurança para os vários setores da sociedade (COM(2016) 410 final).

Em setembro de 2017, a União adota a Comunicação *Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE* onde define um conjunto medidas de maneira a adaptar-

[16] Pelo CNCS, os operadores de serviços essenciais referem-se aos setores de energia, dos transportes, bancário, das infraestruturas do mercado financeiro, infraestruturas digitais, da saúde e do setor do fornecimento e distribuição de água potável. Enquanto, que os prestadores de serviços digitais incluem os serviços de mercados em linha, de pesquisa em linha e de computação em nuvem (CNCS, n.d.).

se melhor ao risco exponencial das ciberameaças, que resultaram em 2017, num impacto económico cinco vezes superior em relação a 2013 (JOIN(2017) 450 final). A União pretende com ela a potencialização das suas estruturas e capacidades a nível da cibersegurança, com a colaboração dos seus países membros.

Jean-Claude Juncker, presidente da Comissão Europeia desde 2014, afirma no seguimento desta proposta que:

> "Os ciberataques podem ser mais perigosos para a estabilidade das democracias e das economias do que armas e tanques (…). Os ciberataques não conhecem fronteiras e ninguém está imune. É por isso que hoje, a Comissão propõe novas ferramentas, incluindo a Agências Europeia de Cibersegurança, para ajudar a defender-nos contra tais ataques" (European Commission, 2017a).

Neste documento, é reforçado o papel da ENISA através de uma proposta de reforma que a tornará mais robusta e eficaz e implicará um mandato permanente para as suas funções, tornando-a no que é atualmente (COM(2017) 477 final). É também sugerida a formulação de um quadro de certificação da cibersegurança a nível da UE que permitirá criar pela primeira vez, um sistema de certificação reconhecido na União, com normas de cibersegurança para os produtos e serviços de TIC e que fará uma avaliação do seu nível de segurança em função do serviço que oferece.

Foi salientada a transposição da Diretiva SRI, por parte dos estados membros, até maio de 2018 e idealizada a construção de uma rede de centros de competências dedicados à cibersegurança nos estados membros, formada em torno de um Centro Europeu de Investigação e de Competências em matéria de Cibersegurança, que pressupõem o "desenvolvimento e a implantação de tecnologias de cibersegurança" e que reforçarão os esforços já realizados pela UE (JOIN(2017) 450 final). Considerou-se também este Centro abranger o domínio da ciberdefesa, área que os estados membros são incentivados a reforçar.

A presente Comunicação engloba também sugestões para o reforço da educação e sensibilização sobre cibersegurança em cursos de formação, tanto nas áreas digitais como noutras, tais como em escolas, em empresas e na administração pública.

É proposta a criação de um plano de ação para a UE e os estados membros no caso de ocorrer um ciberataque em larga escala e um quadro de resposta a crises cibernéticas elaborado pelos estados membros e pelos órgãos da União, por forma a definir como

devem estas entidades reagir eficazmente em situação de incidentes ou crises de cibersegurança em grande escala (Recomendação (UE) 2017/1584 de 13 de setembro).

No mesmo documento, a Comissão finca a importância de uma resposta eficaz do direito penal aos ciberataques, de modo a potenciar os esforços já concretizados na criminalização dos ciberataques. Assim, os estados membros devem elaborar a sua legislação nacional para complementar a jurisdição internacional já criada e a Comissão através da Diretiva *relativa ao combate à fraude e à contrafação de meios de pagamento que não numerário* propõe uma nova atualização na aplicação da lei neste tema (COM(2017) 489 final).

É promovida inclusivamente a cooperação entre a UE e a NATO em termos da cibersegurança e da ciberdefesa, como já vinculado no subcapítulo anterior. Com base nesta reforma de cibersegurança, proposta em setembro de 2017, o Conselho aprova em dezembro de 2018, o Regulamento Cibersegurança com medidas para responder e dissuadir os ciberataques (Conselho Europeu & Conselho da UE, 2019).

Em janeiro de 2018, a ENISA organiza o primeiro exercício de cooperação da rede de *Computer Security Incident Response Team* (CSIRT). Com a participação de vários CSIRT nacionais e da CERT-UE, o exercício visa "o treino dos participantes sobre consciência situacional, partilha de informação, compreensão das funções e responsabilidades e a utilização de ferramentas relacionadas" (ENISA, 2018b). A longo prazo, este exercício tem como objetivo melhorar o nível de cooperação em cibersegurança na UE.

Em fevereiro de 2018, a Agência Europeia de Segurança e Defesa (AESD) responsabiliza-se por criar uma plataforma de educação, formação, avaliação e exercício para a cibersegurança e a ciberdefesa e destaca a necessidade em trabalhar em conjunto com os esforços já realizados pela União neste sentido (Decisão (PESC) 2018/712 de 14 de maio). Esta agência, criada em julho de 2005, tem como missão promover a formação e a educação na União sobre a política comum de segurança e defesa.

Em setembro de 2018, a Comissão propõe o Regulamento que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança, a ser criado de 2021 até 2029, em Bruxelas, e a Rede de Centros Nacionais de Coordenação (SWD(2018) 404). A Rede será constituída após a identificação de entidades públicas ou privadas que trabalham no domínio da cibersegurança, formando os centros de especialização e competências existentes na UE.

Em novembro de 2018, a União adotou o *Quadro Estratégico da UE para a Ciberdefesa*, com atualizações face ao de 2014. Este quadro visa contribuir para a ciberdefesa dos países membros e simultaneamente aumentar a ciberresiliência da União. Nele são apresentados os pontos mais críticos para a ciberdefesa e o papel das entidades europeias que atuam nesta vertente (Conselho da UE, 2018b).

Sumarizando, a UE tem assumido o papel da cibersegurança como um fator determinante para a prosperidade e segurança nacional. Salienta que é da responsabilidade primária de cada membro, assegurar uma segurança e defesa sólidas em questões cibernéticas e que devem continuar a ser promovidas e implementadas medidas eficazes face à constante evolução da cibercriminalidade. Para tal, a UE foi criando ao longo das duas últimas décadas, instrumentos jurídicos, políticas, entidades especializadas, estruturas e cooperações que permitem melhorar a sua capacidade e resiliência, bem como a dos seus países membros, no domínio da cibersegurança e em algumas vertentes da ciberdefesa.

2.3. Portugal

Desde a década de 90, Portugal começou a desenvolver instrumentos que permitissem assegurar um uso mais seguro das TIC. As preocupações demonstradas nesta área pelas organizações que Portugal integra e a informatização dos serviços da Administração Pública no final desta década, foram algumas das razões que impulsionaram o país a produzir e a adotar medidas neste âmbito (Santos, 2014).

Em 1990, foi aprovado o SEGNAC 4 relativo a instruções sobre segurança informática e que atendeu à carência de regulamentação própria para proteger matérias classificadas (RCM n.º 5/90 de 28 de fevereiro). Este documento teve em consideração a evolução dos sistemas informáticos e a dependência que os diferentes setores da sociedade estavam a adquirir em relação à informação que neles corria.

O SEGNAC 4, ainda em vigor, consubstancia-se com o SEGNAC 1, relativo a *instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas*, e o SEGNAC 2, que aprova as *normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação*.

Contudo, só em 1997, surgiu o primeiro documento político, que visava de uma forma muito embrionária, a segurança das redes e dos sistemas de informação, para informações classificadas e não classificadas. O *Livro Verde para a Sociedade da Informação em*

Portugal, contribuiu para uma reflexão estratégica da cibersegurança nacional e teve um papel precursor na construção de medidas e legislação necessárias para responder às exigências da Sociedade da Informação (Portugal, 1997).

Em agosto de 2003, foi aprovado o primeiro Plano de Ação para a Sociedade da Informação, onde a "componente da informação e do conhecimento" tomavam já um "papel nuclear em todos os tipos de atividade humana em consequência do desenvolvimento da tecnologia digital, e da Internet em particular" (RCM n.º 107/2003 de 12 de agosto).

Embora atrasado relativamente às metas propostas pela UE (*e*Europe 2002 e *e*Europe 2005), este Plano tornou-se enriquecedor para a construção da cibersegurança em Portugal. Dentro dos seus objetivos incluía adaptar a sociedade portuguesa como uma Sociedade da Informação toda interligada, determinar "objetivos concretos e concertados entre organismos e entre os setores público e privado" e implementar "mecanismos de monitorização e reporte regular" (RCM n.º 107/2003 de 12 de agosto).

No decorrer dos anos, a cibersegurança e a ciberdefesa passaram a constar da agenda política nacional, criando orientações e iniciativas neste sentido. Todavia, só sensivelmente na última década e com uma forte influência das organizações internacionais, Portugal começou a desenvolver e a colocar em prática mais ações, ferramentas e estruturas, que promovessem a segurança e a defesa do seu ciberespaço e acompanhassem os objetivos propostos pelas organizações.

No ano de 2009, destacou-se a promulgação da Lei do Cibercrime relativa a ataques contra sistemas de informação, que formula as disposições penais materiais, processuais e de cooperação internacional aplicáveis ao cibercrime, baseando-se na Convenção do Cibercrime (Lei n.º 109/2009 de 15 de setembro).

Esta lei veio revogar a primeira Lei da Criminalidade Informática, Lei n.º 109/91 de 17 de agosto, corrigindo algumas lacunas e atualizando-a de acordo com a nova realidade (Santos, 2011). A diferença de quase 20 anos entre ambas, revela a pouca preocupação dada às questões cibernéticas a nível político estratégico no âmbito legislativo nacional, considerando que este tema nesse período foi evoluindo exponencialmente, tendo sido verificada a ocorrência de novos tipos de ameaças e ciberataques realizados a estados como o caso da Estónia, em 2007 e da Geórgia, em 2008.

Em fevereiro de 2012, o governo determina que o Gabinete Nacional de Segurança (GNS) seja responsável por coordenar a consolidação da Estratégia Nacional de Segurança da Informação (ENSI). Um dos objetivos patente nesta estratégia consistia na

criação, instalação e operacionalização de um Centro Nacional de Cibersegurança (RCM n.º 12/2012, de 7 de fevereiro), que passou em 2014 a funcionar no âmbito deste Gabinete.

O GNS é dirigido pela Autoridade Nacional de Segurança (ANS) e tem como incumbências assegurar a segurança de matérias classificadas nacionais ou de organizações internacionais que Portugal integra. É a autoridade de credenciação de pessoas singulares ou coletivas que acedem e manuseiam essas mesmas matérias e é responsável por fiscalizar e inspecionar quem as possui (DL n.º 136/2017 de 6 de novembro).

Em 2013, pela RCM n.º 19/2013, de 5 de abril, é aprovado o Conceito Estratégico de Defesa Nacional (CEDN) e são destacadas a cibersegurança e a ciberdefesa como algumas das prioridades a cumprir com os objetivos da política de segurança e defesa nacional. O ciberterrorismo e a cibercriminalidade foram apontadas como ameaças crescentes à economia e à sociedade, destacando a cibercriminalidade como um dos principais riscos e ameaças à segurança nacional. Neste domínio, estabeleceu-se como ações prioritárias a definição de uma Estratégia Nacional de Segurança do Ciberespaço e o levantamento da capacidade de ciberdefesa nacional.

Baseado no CEDN, o levantamento de uma capacidade de ciberdefesa nacional passou a ser uma das orientações estratégicas em vigor na Defesa 2020, publicada em abril do mesmo ano. A referida reforma define a modelação da Defesa Nacional face aos desafios atuais, com o objetivo de formar umas FFAA mais capacitadas e eficientes (RCM n.º 26/2013 de 11 de abril).

Tendo presente estes dois últimos documentos e tendo em consideração a Estratégia da UE para a Cibersegurança, é publicada em outubro de 2013, a Orientação Política para a Ciberdefesa. O Ministério da Defesa Nacional (MDN) reconhece o ciberespaço como um novo domínio operacional e do qual as FFAA dependem para cumprir de forma eficaz as suas missões.

Esta Orientação apresenta como objetivos "garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques", "assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional" e, por último, "contribuir de forma cooperativa para a cibersegurança nacional" (Despacho n.º 13692/2013 de 28 de outubro).

Igualmente em outubro, Portugal assume a liderança do projeto multinacional de *Smart Defence* da NATO, - *Multinational Cyber Defence Education and Training Project*

(MN CD E&T), que através de atividades de educação e treino em ciberdefesa contribuirá "para melhorar o desenvolvimento das capacidades de Ciberdefesa e a interoperabilidade entre especialistas no âmbito da NATO" (Academia Militar, 2017). Este projeto ocorrerá na NATO *Communications and Information Academy* (NCIA), localizado em Oeiras e visa ministrar treino especializado em sistemas avançados de TIC e sistemas cibernéticos da NATO, a pessoal civil e militar, tanto da própria Aliança como dos seus membros (NCIA, 2017).

No ano de 2014, o Centro Nacional de Cibersegurança (CNCS) inicia serviço no âmbito do GNS e com a missão de "contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura" (DL n.º 69/2014 de 9 de maio). O CNCS exerce as suas competências como coordenador operacional e autoridade nacional em cibersegurança em função do Estado, das infraestruturas críticas nacionais, dos serviços essenciais e dos serviços digitais. Para tal, conta com diversas medidas e meios que permitam prever, detetar, responder e recuperar de um estado originado por um ciberincidente ou ciberataque.

Este Centro integra o CERT.PT, que constitui um serviço responsável por coordenar uma resposta face a ciberincidentes que ocorram no ciberespaço nacional, ou seja, que envolvam o Estado ou os operadores mencionados em cima. Este serviço está inserido na Rede Nacional de CSIRT, que por sua vez coopera com a Rede Europeia de CSIRT, determinado pela Diretiva (EU) 2016/1148. Os objetivos da CSIRT nacional são essencialmente colaborar de forma eficaz com os países membros da UE e promover uma maior segurança cibernética nacional.

O CNCS atua igualmente em "articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo" (DL n.º 69/2014 de 9 de maio). Compete exclusivamente às FFAA a capacidade de ciberdefesa nacional, sem excluir a sua contribuição e cooperação para a cibersegurança nacional.

Em setembro de 2014, é procedida a primeira alteração à Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA), aprovada pela Lei Orgânica n.º 1-A/2009, de 7 de julho. Pela presente lei é ressalvado o papel das FFAA portuguesas como um "pilar essencial da defesa nacional" e com a missão de "garantir a defesa militar da República" (Lei Orgânica n.º 6/2014 de 1 de setembro). É aprovado ainda o funcionamento do Centro de Ciberdefesa (CCD) como uma das competências do CEMGFA.

Neste seguimento, é aprovado em dezembro de 2014, a nova orgânica do Estado-Maior General das Forças Armadas (EMGFA) que determina a aprovação da estrutura interna do EMGFA por decreto regulamentar (DL n.º 184/2014 de 29 de dezembro). Desta forma, é publicado o Decreto Regulamentar n.º 13/2015, de 31 de julho, que estabelece a missão e estrutura da Direção de Comunicações e Sistemas de Informação (DIRCSI), compreendida no EMGFA e chefiada pelo CEMGFA.

A DIRCSI[17] tem competências no âmbito da ciberdefesa e na cibersegurança setorial da defesa nacional, onde tem por missão "coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação" das FFAA e do restante universo da defesa nacional, respetivamente (DR n.º 13/2015 de 31 de julho).

A DIRCSI compreende na sua estrutura o CCD a quem compete "assumir a direção e coordenação da capacidade nacional de ciberdefesa", colaborar com o CNCS e com os CIRC nacionais e internacionais e "exercer a autoridade técnica no âmbito da ciberdefesa e da cibersegurança setorial da defesa nacional", entre outras (DR n.º 13/2015 de 31 de julho). O CCD iniciou serviço em 2015 e é responsável por coordenar e colaborar com os Núcleos CIRC dos três ramos das FFAA.

Pouco antes de ser publicado o anterior Decreto Regulamentar, é aprovada em junho, a Estratégia Nacional de Segurança do Ciberespaço (ENSC). A Estratégia, denominada doravante desta forma, definia os objetivos e as linhas de ação, a nível nacional, com a finalidade de melhorar o nível de segurança das redes e da informação. Sobre os pilares da subsidiariedade, da complementaridade, da cooperação, da proporcionalidade e da sensibilização, foram definidos os seus objetivos estratégicos através de seis eixos de intervenção[18] (RCM n.º 36/2015 de 12 de junho).

A Estratégia previu uma avaliação anual do cumprimento dos seus objetivos estratégicos e das linhas de ação, orientada pelo Conselho Superior de Segurança do Ciberespaço (CSSC), bem como a sua adaptação aos desafios impostos pela evolução digital. O CSSC foi criado com a missão de "assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da ENSC e da respetiva revisão" (RCM n.º 115/2017 de 24 de agosto). Este Conselho é constituído por representantes das diferentes entidades com responsabilidades na segurança do

[17] Ver em Anexo A, a missão, estrutura e competências da DIRCSI e do CCD.
[18] Ver em Anexo B, a transcrição dos pontos mais relevantes da ENSC 1.0.

ciberespaço nacional, conforme estabelecido no Eixo 1 – *Estrutura de segurança do ciberespaço* da ENSC.

De acordo com o Relatório de Avaliação Final de 31 de maio de 2018, verificou-se que nos anos de 2016, 2017 e 2018 e de um modo geral nos seis eixos de intervenção da Estratégia, existiu um aumento do número de atividades (71, 101 e 121, respetivamente), do número de tarefas executadas (7, 54 e 71, respetivamente) e do número de tarefas em execução (46, 45 e 49, respetivamente). Os dados retirados da avaliação dos três anos evidenciam o comprometimento das várias entidades responsáveis em cumprir as linhas de ação definidas pela Estratégia e mostram resultados positivos na sua concretização.

No entanto, as "medidas e atividades da ENSC são (…) genéricas e de grande amplitude, podendo ser alcançadas de forma distintas" (GNS/CNCS, 2018). Este fator tem de positivo a liberdade de ação das diferentes entidades para a adoção das medidas e atividades que melhor se adequam à respetiva instituição, organização ou empresa. Contudo, questiona-se se as mesmas não criam ambiguidade, tornando a sua avaliação demasiado abrangente para efetuar um controlo eficaz da operacionalização das medidas e atividades criadas.

Uma das linhas de ação na Estratégia é a participação em exercícios por "permitirem a avaliação e o desenvolvimento de capacidade doutrinárias e operacionais" (RCM n.º 36/2015 de 12 de junho). Neste sentido, a ENSC 1.0 incentivava as diferentes entidades a participarem em exercícios de segurança e defesa do ciberespaço, nacionais e no contexto da NATO e da UE.

Desde 2010 que Portugal participa no *Cyber Europe*, organizado pela ENISA, de dois em dois anos, para entidades a nível da UE. Este exercício "contempla incidentes técnicos inspirados na vida real, que produzirão situações de crise ao nível local, organizacional, nacional e europeu" (CNCS, 2018b). Portugal participa com várias entidades, entre os quais o CNCS, enquanto autoridade nacional de cibersegurança, e a ANACOM, enquanto autoridade nacional de comunicações.

No contexto da NATO, Portugal participa no "maior exercício de ciberdefesa da NATO", o *Cyber Coalition*, com o principal objetivo de "treinar as equipas de ciberdefesa das Nações aliadas e parceiras, na prevenção e reação a ataques cibernéticos contra sistemas nacionais e NATO" (EMGFA, 2018b). Portugal iniciou a sua participação em 2011, com as FFAA, e em 2015 com o CCD.

Igualmente desde 2011, o Exército organiza todos os anos, o Ciber Perseu que "se destina a avaliar a capacidade de resposta do Exército face à ocorrência de ciberataques

de âmbito nacional e internacional que podem escalar para uma crise no ciberespaço" (Exército Português, 2018). Esta série de exercícios conta com a participação do MDN e das FFAA, bem como dos setores público e privado, a indústria e outras organizações/empresas que tencionem participar. A colaboração com entidade externas resulta da "consciência que a eficácia das ações de defesa do ciberespaço depende, fundamentalmente, da atuação sinérgica e colaborativa da sociedade portuguesa" (Exército Português, 2018).

Em janeiro de 2018, Portugal participou no *Cyber SOPEx*, o primeiro exercício organizado pela ENISA e dirigido à rede CSIRT. Várias equipas da CSIRT nacionais e da CERT-UE, incluindo o CERT-PT, participaram neste exercício, que visa melhorar a cooperação entre as equipas de resposta a incidentes de segurança informática (CNCS, 2018a).

Portugal participa ainda no exercício *Locked Shields*, desde 2018, organizado anualmente pelo CCD COE. Este exercício ocorre com base em cenários reais e permite aos vários participantes aprimorar as suas capacidades de "defesa dos sistemas nacionais de TI [Tecnologias de Informação] e das infraestruturas críticas sob ataques em tempo real" (CCDCOE, 2019).

Segundo notícia do EMGFA, o "maior e mais complexo exercício de ciberdefesa internacional" visa preparar os participantes para "responderem a incidentes ao nível técnico, que terão impacto direto no nível operacional de condução de uma operação militar, bem como ao nível de decisão estratégica" (EMGFA, 2019). Este exercício envolve as FFAA, com a coordenação do CCD, uma equipa de apoio jurídico às operações no ciberespaço e o CNCS "enquanto parceiro privilegiado para a garantia da segurança do ciberespaço", entre poucos mais participantes.

A participação do país neste exercício decorre da sua adesão ao CCDCOE, em abril de 2018. Esta organização militar internacional conta com 20 nações e direciona-se para a pesquisa, treino e exercícios na área da ciberdefesa. A presença de Portugal no Centro da NATO, após a sua nota de adesão ao Memorando de entendimento (MoU) pelo MDN (Despacho n.º 9762/2017 de 9 de novembro), permite melhorar a capacidade nacional de ciberdefesa.

Segundo notícia do EMGFA, esta adesão permite reforçar "a ligação com o novo domínio de operações militares e potenciar um maior conhecimento situacional das evoluções que decorrem na Aliança nesta área" (EMGFA, 2018a). Além disto, possibilita

a reafirmação do "comprometimento nacional com o *Cyber Defence Pledge*, que foi assumido (…) na cimeira de Varsóvia, em 2016".

Em 2018, iniciou-se também a primeira edição do Exercício Nacional de Cibersegurança (ExNCS), com uma periodicidade anual e como previsto nas atividades da ENSC. O GNS/CNCS é a entidade responsável por organizar este exercício e conta com a participação dos setores público e privado, nomeadamente o CCD, o CNCS e a ANACOM, entre outras, para a resolução de incidentes no ciberespaço baseado em vários cenários reais (CNCS, 2019).

Em abril de 2018, é divulgada para as FFAA, a Diretiva Estratégica do EMGFA 2018-2021 que define os objetivos estratégicos e respetivas linhas de ação a cumprir para o período indicado. A Diretiva intenta à "permanente adaptação aos desafios decorrentes de fatores externos e [a] uma melhoria contínua do desempenho interno, à luz das circunstâncias da organização, tendo em vista garantir a relevância e a utilidade da Instituição Militar para Portugal e os Portugueses" (*Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2018-2021*, 2018).

No presente documento, o EMGFA reconhece a deficiente capacidade que as FFAA têm para "fazer face aos desafios do mundo digital, designadamente das ciberameaças" e inclui nas ameaças ao país os ciberataques aos países da Aliança Atlântica e o impacto que estes podem ter a nível nacional ou global. No entanto, afirma que a "transferência de conhecimento e tecnologia C4ISR[19] e ciberdefesa, com a instalação da Academia de Comunicações e Informação da NATO, em Oeiras" é uma oportunidade para as FFAA e, inclusivamente, para Portugal. Deste modo, é estabelecido como um dos objetivos estratégicos a edificação da capacidade de ciberdefesa nacional.

No seguimento da Diretiva Estratégica do EMGFA, formou-se um grupo de trabalho (GT-CCFA)[20] responsável por elaborar o Plano de Desenvolvimento da Capacidade de Ciberdefesa[21], apresentado em dezembro do mesmo ano. Este plano estratégico visa a melhoria e o desenvolvimento das capacidades das FFAA ao nível da ciberdefesa, tanto

[19] *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*.
[20] A nível político, a Orientação Política para a ciberdefesa, em 2013, e a Diretiva Ministerial de Orientação Política para o Investimento na Defesa, em 2018, foram também razões para a criação deste Grupo de Trabalho. Este grupo de trabalho constituiu-se com especialistas do EMGFA, dos ramos das FFAA e do MDN.
[21] A sua elaboração teve em consideração os modelos adotados por países aliados para a sua capacidade de ciberdefesa, uma vez que têm mais experiência na área. Foram então considerados a Espanha, a França, a Roménia, o Reino-Unido, a Itália, a Alemanha e os Estados-Unidos.

na defesa das suas redes militares contra ataques cibernéticos, como na condução de operações militares neste novo domínio (GT-CCFA, 2018).

Em conformidade com este plano e com as especificidades de cada ramo, foi formulado por cada grupo de trabalho respetivo, o seu plano de ação no âmbito da ciberdefesa. Especificamente para a Marinha, foi o Grupo de Trabalho do EMA (GT-EMA), a quem competiu a elaboração do Plano de Ação para o Reforço da Ciberdefesa da Marinha.

Em maio de 2018, entrou em vigor o Regulamento Geral de Proteção de Dados (RGPD) que define um conjunto de regras de proteção de dados para todas as empresas na UE, independentemente da sua localização[22]. O RGPD visa garantir a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e da sua circulação (Regulamento (UE) 2016/679, de 27 de abril). Neste sentido, em 2019, foi aprovada a Lei n.º 58/2019, de 8 de agosto, que visa "[assegurar] a execução, na ordem jurídica nacional" deste mesmo regulamento (Lei n.º 58/2019 de 8 de agosto).

Em agosto de 2018, foi aprovada a primeira lei que estabelece o regime jurídico da segurança do ciberespaço e que transpõe a Diretiva (UE) 2016/1148, de 6 de julho, *relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*. A presentei lei aplica-se à administração pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais e aos prestadores de serviços digitais, bem como a todas as outras entidades que utilizem redes e sistemas de informação (Lei n.º 46/2018 de 13 de agosto).

No corrente ano, foi aprovada em Conselho de Ministros, em 23 de maio de 2019, e para o período de 2019-2023, a Estratégia Nacional de Segurança do Ciberespaço 2.0[23], que revoga a sua primeira versão (Conselho de Ministros, 2019). Desenvolvida pelo CSSC e tendo sido publicada no Diário da República através da RCM n.º 92/2019, de 5 de junho, este Conselho teve em consideração a evolução digital sentida desde 2015 e pela qual foi realizada a primeira Estratégia. A sua execução "permitirá tornar Portugal um país mais seguro, através de uma ação inovadora e resiliente que preserve os valores fundamentais do Estado de Direito e garanta o regular funcionamento das instituições" (RCM n.º 92/2019 de 5 de junho).

[22] O RGPD foi retificado no Jornal Oficial da UE, em maio de 2018 (Jornal Oficial da UE, 2018).
[23] Ver em Anexo C os pontos mais relevantes da ENSC 2.0.

A implementação da ENSC 2.0, será verificada pelo CSSC, tal como estipulado pela Lei n.º 46/2018, de 13 de agosto, e é acompanhada do respetivo Plano de Ação, que deverá ser elaborado no prazo de 120 dias desde a sua entrada em vigor, dia 6 de junho de 2019.

A ENSC 2019-2023 constitui-se um "instrumento estruturante para a capacitação nacional" no âmbito da segurança do ciberespaço (RCM n.º 92/2019 de 5 de junho). Com este pressuposto, através da definição dos seus objetivos estratégicos, transpuseram-se pelos seis eixos que a compõem, determinadas orientações "destinadas a reforçar o potencial estratégico nacional no ciberespaço através do incremento da sua segurança".

Os seus objetivos estratégicos traduzem-se na maximização da "resiliência digital nacional" para "salvaguardar a segurança do ciberespaço de interesse nacional", na promoção da inovação através do ciberespaço enquanto "domínio de desenvolvimento económico, social, cultural e de prosperidade" e, por último, em "gerar e garantir recursos (…) adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço" (RCM n.º 92/2019 de 5 de junho).

Em relação à primeira versão, destaca-se a definição de um Plano de Ação que permitirá às diversas entidades empenhadas responder de um modo mais assertivo às linhas orientadoras expressas ao longo dos diferentes eixos de intervenção. Numa primeira análise, este requisito colmata a questão levantada anteriormente ao longo da apresentação da ENSC 1.0. Sendo ela a possível ambiguidade e existência de erros nas ações a tomar, bem como a respetiva incorreta avaliação, originada pela generalidade e grande abrangência das medidas e atividades definidas pela ENSC 1.0.

Na contextualização da Estratégia em vigor, são apontados diversos fatores que dificultam a eficácia da segurança do ciberespaço nacional. Sem excluir as vulnerabilidades associadas às características envolventes do mesmo, são identificadas como principais fragilidades a "fraca cultura de cibersegurança e de consciência das responsabilidades individuais" e a "insuficiente maturidade digital para atender às necessidades de segurança" nos setores público e privado (RCM n.º 92/2019 de 5 de junho).

Além desta realidade, "a dificuldade de capacitação, manutenção e captação de recursos humanos e financeiro que permitam o acompanhamento da rápida evolução tecnológica" (RCM n.º 92/2019 de 5 de junho) é apresentada como mais uma vulnerabilidade a nível nacional.

Em suma, Portugal tem revelado comprometimento na definição e adoção de medidas que permitam salvaguardar e garantir a segurança do ciberespaço através de uma estrutura

nacional de cibersegurança e ciberdefesa constituída por vários organismos. Admite-se que esta estrutura é "imprescindível em sociedades baseadas/dependentes da Informação", o que atualmente se torna imperativo tanto no quadro na UE, como da NATO (Viana, 2018).

Embora com os esforços sentidos a nível nacional e com a colaboração e apoio das organizações a que pertence, é possível afirmar que Portugal ainda não se encontra totalmente adaptado à evolução tecnológica sentida, destacando-se a importância das medidas e atividades neste âmbito serem revistas e atualizadas conforme a evolução do ciberespaço e das suas ameaças, criando ainda métodos que permitam contornar ou combater as principais vulnerabilidades destacadas a nível nacional.

3. Cibersegurança na Marinha Portuguesa

Com base no exposto no subcapítulo anterior, destacam-se como fatores evolutivos para a capacidade de cibersegurança da Marinha: a ENSC, através das medidas impostas pela sua primeira versão e pelas atualizações decorrentes da sua versão mais recente; a Lei n.º 46/2018, de 13 de agosto, como a primeira lei que estabelece o regime jurídico da segurança do ciberespaço; e o Plano de Ação para o Reforço da Ciberdefesa da Marinha, de acordo com o definido no Plano de Desenvolvimento da Capacidade de Ciberdefesa para as FFAA.

Os esforços exercidos, tanto pelas anteriores organizações, como por Portugal, nesta vertente da segurança, revelam a necessidade de um trabalho conjunto das várias partes. A criação de doutrina ou a formação do pessoal e a educação dos operadores finais, entre outros, constituem componentes de igual forma essenciais.

Do mesmo modo, a edificação e o desenvolvimento de uma capacidade operacional na Marinha Portuguesa envolve diferentes componentes também interdependentes e coordenados. Segundo a NATO, "as lacunas de uma capacidade são mitigadas por qualquer combinação de doutrina, organização, treino, material, desenvolvimento de liderança, pessoal, instalações e soluções de interoperabilidade" (NATO, 2019).

Com este pressuposto, a análise da atual capacidade de cibersegurança da Marinha será baseada na metodologia DOTMLPI-I[24] (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade), composto pelos pilares necessários à edificação de uma capacidade operacional.

3.1. Doutrina

A Doutrina consiste em princípios fundamentais que visam a coordenação de meios para o cumprimento de objetivos e é caracterizada por ser autoritária, mas simultaneamente exigir deliberação na sua aplicação (NATO, 2019). Os princípios fundamentais presentes nesta dimensão devem definir os objetivos e o âmbito de aplicação da mesma.

[24] Acrónimo criado pelo Departamento de Defesa dos EUA e adotado, mais tarde, pela NATO.

Como doutrina, a Marinha utiliza diplomas legais, estratégias e políticas, muitas dos quais já mencionados no capítulo anterior. A sua utilização permite a diminuição da ambiguidade na tomada de decisão e nas ações a realizar, enquanto aumenta a eficácia a nível da cibersegurança (Neves & Correia, 2016).

A nível nacional, a doutrina com maior utilidade prática para a Marinha, que regula juridicamente e define uma estratégia de ação na vertente da cibersegurança, baseia-se na Lei n.º 46/2018, de 13 de agosto e na Estratégia Nacional de Segurança do Ciberespaço (ENSC)[25], respetivamente.

Para a organização da sua estrutura interna e respetivas competências, a Marinha rege-se pelo Decreto Regulamentar n.º 10/2015, de 31 de julho, exposto no subcapítulo da Organização. Ainda a nível interno, para a segurança da informação, das redes e dos seus SIC, a atuação da Marinha concentra-se, de um modo geral, nas seguintes publicações:

- PCA 2 – Doutrina para os Sistemas de Informação e Comunicação Automatizados (SICA) na Marinha;
- PCA 3 - Política de segurança para interligação de redes e sistemas de informação e comunicação automatizados;
- PCA 10 - Conceito de implementação dos sistemas de informação e comunicação automatizados (SICA) no domínio do utilizador;
- PCA 15 - Doutrina para a Intranet e Internet na Marinha;
- PCA 16 - Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha.

Entre as quais, a última por ser a publicação base para a ciberdefesa na Marinha, tem uma maior relevância para o teor deste estudo. Num esforço de complementar a doutrina empregue na Marinha, é utilizada eventualmente e em caso de necessidade, doutrina tanto da NATO, como da UE.

Internamente, de acordo com as referências doutrinárias supracitadas, os PCA (Publicações de Comunicações da Armada) são publicações escritas como documentos enquadradores dos referentes temas. Neste sentido, pode-se afirmar que a Marinha não possui "formalmente nenhuma Doutrina aprovada", mas sim "um conjunto de publicações doutrinárias do EMA [Estado-Maior da Armada]" (Neves, 2019)[26].

[25] A Lei e a ENSC, com as versões 1.0 e 2.0, foram introduzidas anteriormente no subcapítulo *Portugal*, em contexto nacional. No presente capítulo serão abordadas relativamente às FFAA/Marinha.
[26] Ver Apêndice C – Entrevista ao Comandante Baptista das Neves (NCIRC).

Ainda segundo a mesma fonte, é "fundamental a existência de doutrina operacional para a utilização do ciberespaço, até agora inexistente quer na Marinha quer nas Forças Armadas". Embora este conceito pressuponha especialmente uma presença ativa da Marinha no ciberespaço e o presente trabalho não seja focado nessa vertente da ciberdefesa, importa referir este fator. Inerentemente, concilia-se com o domínio da cibersegurança da própria organização e simultaneamente, enquanto ramo das FFAA, a Marinha atua no domínio da ciberdefesa.

Neste sentido, a doutrina não deverá só responder a essa necessidade, como deverá também assegurar que os princípios fundamentais que deverão reger a organização sejam inteligíveis, garantindo igualmente o seu alinhamento com o CCD e os seus aliados (Carvalho, 2019; Prates, 2019)[27].

3.1.1. Estratégia Nacional de Segurança do Ciberespaço (ENSC)

A Estratégia 1.0 visou, a nível nacional, garantir eficazmente a segurança das redes e da informação, através da execução de certos objetivos estratégicos e consequentes eixos de intervenção[28]. No Eixo 1 - *Estrutura de segurança do ciberespaço*, foi definida a medida de desenvolver a capacidade de ciberdefesa através das seguintes linhas de ação:

"a) Concretizar a Orientação Política para a Ciberdefesa (…) edificando a estrutura de ciberdefesa nacional;

b) Estabelecer e consolidar uma estrutura de comando e controlo da ciberdefesa nacional (…);

c) Implementar, desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço (…);

d) Constituir a ciberdefesa uma área onde é necessário promover sinergias e potenciar o emprego dual das suas capacidades, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão" (RCM n.º 36/2015 de 12 de junho).

[27] Ver Apêndice D – Entrevista ao Comandante Caldeira Carvalho (EMA) e Apêndice E – Entrevista ao Engenheiro Marques Prates (EMA).
[28] Em Anexo B encontram-se os pontos mais relevantes da ENSC 1.0.

Tal como questionado no subcapítulo referente a Portugal relativamente à aplicação da Estratégia a nível nacional, levanta-se a mesma dúvida na sua aplicação específica para as FFAA.

A grande variedade de formas com que as FFAA podem cumprir com as linhas orientadoras definidas na Estratégia 1.0 permite uma maior liberdade de escolha nas medidas e atividades que melhor se adequam à organização. Contudo, a mesma situação pode criar ambiguidade nas ações a tomar e suscitar dúvidas ou erros na sua aplicação.

A Estratégia 1.0 demonstrou a falta de um plano de ação claro, onde deveriam ser definidos certos parâmetros que fossem de encontro às medidas estabelecidas na Estratégia (Jesus, 2019)[29]. Neste sentido, a nova Estratégia (ENSC 2.0) irá incluir um Plano de Ação, com indicadores e metas orientados para o cumprimento de cada medida estabelecida na ENSC 2.0 e que permitirá combater os constrangimentos acima referidos (Marques, 2019; Jesus, 2019)[30].

De acordo com a Estratégia 1.0 e com as linhas de ação referidas pela mesma, a atuação das FFAA é salientada enquanto organismo responsável pela ciberdefesa nacional e é nesse âmbito que vão de encontro as atividades propostas pelo MDN/EMGFA. No entanto, existem outros eixos de intervenção e respetivas medidas concretas que se adequam igualmente às FFAA enquanto organização. Torna-se exemplo disso o Eixo 4 – *Educação, sensibilização e prevenção*, que pode ser considerado um eixo relevante e comum a todas as entidades que utilizam o ciberespaço, mas onde não estão vertidas ações para a Defesa.

A ausência da atribuição de certas medidas e atividades associadas aos restantes eixos, pode revelar pela Estratégia 1.0, um deficiente desenvolvimento da capacidade de ciberdefesa das FFAA e inerentemente, da Marinha. Por essa razão, a ENSC 2.0 já prevê a atuação da Defesa em todos os seus seis eixos (Marques, 2019; Jesus, 2019), transpondo-se numa contribuição mais sólida e eficaz para o desenvolvimento da cibersegurança na Marinha.

A Estratégia 2.0, aprovada para o período de 2019-2023 e desenvolvida pelo CSSC, considerou na sua formulação a evolução digital ocorrida desde a publicação da sua primeira versão. Como supracitado, a ENSC 2.0 contempla um Plano de Ação, que deve

[29] Disponível em Apêndice B – Entrevista ao Comandante Fialho de Jesus (CCD).
[30] Disponível em Apêndice A – Entrevista ao Almirante Gameiro Marques (GNS/ANS).

ser elaborado até ao 120.º da entrada em vigor da resolução a que diz respeito (RCM n.º 92/2019 de 5 de junho).

Nesta última versão distingue-se a adaptação dos seis eixos de intervenção à exigência atual da segurança do ciberespaço, tendo sido consideradas novas vertentes para os mesmos[31]. Neste sentido, as linhas orientadoras que compõem cada eixo, introduzem ações especificamente para as FFAA no Eixo 1 – *Estrutura de segurança do ciberespaço*, no Eixo 3 – *Proteção do ciberespaço*, no Eixo 4 – *Resposta às ameaças e combate ao cibercrime* e no Eixo 6 – *Cooperação nacional e internacional*.

Embora não se particularize no Eixo 2 – *Prevenção, educação e sensibilização* e no Eixo 5 – *Investigação, desenvolvimento e inovação* a sua aplicação às FFAA, são incluídas diversas medidas que podem ser tidas em conta, especialmente no primeiro eixo, considerando ainda que é um dos mais relevantes na eficácia da respetiva Estratégia. Neste âmbito, a sua aplicabilidade às FFAA poderá ser preconizada tanto como organização, como entidade com responsabilidade na segurança do ciberespaço.

3.1.2. Lei n.º 46/2018, de 13 de agosto

A Lei n.º 46/2018, de 13 de agosto, estabelece, para todas as entidades que utilizem redes e sistemas de informação, o regime jurídico da segurança do ciberespaço. No entanto, para a sua aplicabilidade na Marinha, esta exclui as redes e os sistemas de informação[32] relacionadas diretamente com o Comando e Controlo (C2) do EMGFA e dos respetivos ramos, bem como os que processam informação classificada (n.º 6 do Art.º 2.º, Lei n.º 46/2018 de 13 de agosto).

As redes e os sistemas de informação ligados ao C2 são todos os que se relacionam diretamente com a "autoridade, responsabilidade e atividade do Comandante em dirigir e coordenar as forças militares e na implementação das ordens relacionadas com a execução das operações" (EMA, 2005). No segundo caso, são consideradas as redes e os sistemas de informação que processam toda a informação que "se for do conhecimento de pessoas

[31] Em Anexo C encontram-se os pontos mais relevantes da ENSC 2.0, considerando as linhas orientadoras específicas para as FFAA ou que poderão incluir ações para esta organização.
[32] Para efeito da presente lei, o conceito "rede e sistema de informação" é assumido como "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede de comunicações eletrónicas que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção" (Lei n.º 46/2018 de 13 de agosto).

não autorizadas, pode fazer perigar a segurança nacional, dos países aliados ou de organizações de que Portugal faça parte" (GNS, n.d.).

Neste contexto, torna-se pertinente mencionar as atribuições da DIRCSI, com missão nas "atividades inerentes aos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) necessários ao exercício do comando e controlo nas Forças Armadas" (N.º 1, Art.º 30.º, DL n.º 184/2014 de 29 de dezembro).

A missão da DIRCSI é definida no âmbito da ciberdefesa e da cibersegurança setorial da Defesa Nacional, salientando-se que especifica a segurança e a defesa das redes das FFAA como ciberdefesa e das restantes redes da Defesa Nacional como cibersegurança setorial. Visando em ambas a coordenação da "proteção dos valores da integridade, confidencialidade de disponibilidade" da respetiva informação e sistemas de informação (N.º 2 e 3, Art.º 30.º, DL n.º 184/2014 de 29 de dezembro).

Segundo o exposto da Lei e do Decreto-Lei referidos acima, questiona-se se poderá ser considerada uma sobreposição de competências da DIRCSI aos poderes de autoridade da Autoridade Nacional de Cibersegurança (ANC) sobre as redes e sistemas de informação da Defesa que não as excluídas na Lei n.º 46/2018, de 13 de agosto.

Pelo definido na presente lei, a Marinha deve "cumprir as medidas técnicas e organizativas adequadas e proporcionais" de modo a prevenir os riscos e evitar os incidentes que comprometem a segurança das suas redes e sistemas de informação, devendo estas medidas ser proporcionais ao risco em causa (Art.º 14.º, Lei n.º 46/2018 de 13 de agosto). O Art.º 15.º da mesma lei, estabelece que na ocorrência de um incidente com impacto relevante nas redes e sistemas de informação, a Marinha deve notificar o CNCS.

Tanto os requisitos de notificação de incidentes, como os requisitos de segurança, deveriam ter sido definidos em legislação própria, após 150 dias da entrada da lei, ou seja, no primeiro mês de 2019, o que não se verificou até ao momento de realização deste trabalho. Estes pontos encontram-se vertidos num dos objetivos da ENSC 2.0, de modo a "assegurar um enquadramento legal claro para todos" (RCM n.º 92/2019 de 5 de junho).

3.1.3. PCA 16 - Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha

O PCA 16 tem por fim "responder de forma concertada a incidentes de segurança da informação, relacionados com atividades de software malicioso, atividades maliciosas, negação de serviços, ou outras ameaças/vulnerabilidades inerentes aos SICA" (Sistemas de Informação e Comunicação Automatizados) (EMA, 2012). A relevância destes sistemas para a Marinha, prende-se com a sua função de armazenagem, processamento e transmissão de informação sensível, para fins operacionais e administrativos, e que podem comprometer a defesa dos seus recursos no ciberespaço.

Desta forma, o PCA 16 definiu e permitiu a implementação da Capacidade de Resposta a Incidentes de Segurança da Informação (CRISI)[33] na Marinha, consubstanciada através de uma "organização estruturada, em processos e tecnologias" e orientada para todos os SICA[34] da Marinha e a sua comunidade de utilizadores. O seu principal objetivo é "prevenir e diminuir o risco de ocorrência de incidentes de segurança da informação e minimizar o seu impacto nos SICA, garantindo uma resposta adequada" (EMA, 2012).

No entanto, o PCA 16 foi promulgado em 2012, desde o qual já passaram pelo menos sete anos num contexto situacional em constante evolução e a um ritmo acelerado. No mesmo período, por forma a dar resposta às novas ciberameaças, foram publicadas orientações da NATO e da UE, bem como doutrina específica de ambas as organizações, que se traduziram em orientações do EMGFA e, por conseguinte, do EMA, capazes de complementar e tornar mais eficaz a atual CRISI. Entretanto, foram ainda criadas estruturas em Portugal, tais como o CNCS e o CCD, reformulando também elas a organização da CRISI na Marinha.

Com esta realidade presente, o GT-EMA, responsável por elaborar o Plano de Ação para o Reforço da Ciberdefesa da Marinha, considera tanto o PCA16, como as restantes

[33] A CRISI resultou do definido em diretivas internas (Diretiva da Política Naval) e em recomendações da NATO (Declaração de Praga, de 21 de novembro de 2002; Conceito Estratégico de Defesa e Segurança da NATO, de 19 de novembro de 2010; e Cimeira da NATO em Lisboa, de 20 de novembro de 2010) e da UE (Estratégia interna da UE).
[34] Os SICA da Marinha incluem a Infraestrutura tecnológica da Marinha, a rede NSWAN, as redes de missão, a rede MMHS, a Intranet, a Internet e outras redes públicas e as redes móveis.

publicações para o domínio dos sistemas de informação[35], muito desatualizadas e carecidas de uma profunda revisão (GT-EMA, 2018).

A revisão do PCA16 é assumida como prioritária e deve ser rapidamente alinhada com a doutrina NATO e as orientações a nível nacional. Com a consciência de que as ciberameaças se caracterizam pela sua constante mutação e revelam uma adaptação célere às barreiras de proteção impostas, o GT-EMA reconhece que a atualização da doutrina deve ser um processo contínuo.

3.2. Organização

A Organização consiste no modo como é coordenada uma estrutura por forma a cumprir uma missão ou tarefa atribuída (NATO, 2018a). Esta estrutura é suportada por unidades operacionais, equipas e, por último, em indivíduos, sendo que o sucesso das missões e tarefas depende bastante da sua organização, realçando-se a articulação e a comunicação dentro da mesma (Neves & Correia, 2016).

Na organização da Marinha, existe uma estrutura a quem compete a segurança do ciberespaço e da informação, permitindo assegurar uma resposta a incidentes que ocorram nesta dimensão. Os órgãos que formam esta estrutura possuem diferentes níveis de atuação e articulam-se de acordo com as respetivas competências.

A um nível estratégico e com responsabilidades na coordenação encontra-se o Estado-Maior da Armada (EMA), órgão de apoio à decisão do Chefe de Estado-Maior da Armada (CEMA). O EMA compreende a Divisão de Operações que por sua vez, inclui o Núcleo de Ciberdefesa e Tecnologias de Informação e Comunicações[36] (Despacho do Almirante CEMA, n.º 59/18 de 11 de dezembro). É a este nível que compete a elaboração de doutrina em matéria da segurança e defesa do ciberespaço e da informação, a coordenação das ações da Marinha no mesmo domínio e o estabelecimento do contacto com entidades externas.

O EMA é apoiado juridicamente pelo Departamento Jurídico Operacional e Internacional (DJOI), aprovado pelo Despacho do CEMA n.º 35/2007, de 6 de julho. A

[35] Como exemplo, o PCA 2 (B), o PCA 15, o PDA 3 - Política de Gestão da Informação na Marinha e o PCA 12 (A) - Conceito de implementação dos sistemas de informação e comunicação automatizados (SICA) no domínio da rede, datam de 2005, 2010, 2008 e 2012, respetivamente.
[36] A referida divisão e respetivo núcleo foram criados por motivos de necessidade de reajuste da estrutura do EMA resultante do envolvimento da Marinha em vários projetos, como o da edificação e consolidação da Capacidade de Ciberdefesa na Marinha.

DJOI possui incumbências no "[estudo e no tratamento] das matérias relacionadas com o Direito do Mar e o Direito dos Conflitos Armados", emitindo pareceres "sempre que solicitado" .

Na coordenação ao nível operacional, o Comando Naval (COMNAV) é a entidade com responsabilidade nesse âmbito. Neste sentido, pelo regulamentado, compete ao COMNAV "coordenar as atividades de ciberdefesa no âmbito das operações navais" e "planear e coordenar o treino das forças e unidades operacionais na área da ciberdefesa" (*Regulamento Interno do Comando Naval*, 2016).

Abordando o conceito da ciberdefesa ao nível das operações de ataque e de exploração, a Marinha não possui ainda capacidade para atuar neste sentido, sendo o seu papel centrado na defesa dos sistemas de informação internos e periféricos (Quaresma, 2019; Neves, 2019; Carvalho, 2019; Prates, 2019)[37]. Ainda assim, o papel do COMNAV neste âmbito é ainda muito primitivo.

Pelo DR n.º 10/2015, de 31 de julho, é regulamentada a Superintendência das Tecnologias da Informação (STI), órgão central de administração e direção da Marinha (OCAD)[38], responsável "pela segurança da informação e do ciberespaço, pela governação dos sistemas de informação, pelo controlo da configuração das redes e pela gestão do parque informático".

Exerce competências enquanto coordenador técnico da CRISI e órgão de ligação com o EMA, tendo como incumbência "definir a arquitetura de segurança do ciberespaço controlado pela Marinha e dirigir os serviços destinados a garantir a segurança e defesa desse espaço, em articulação com as demais estruturas da Marinha e com o Centro de Ciberdefesa".

A STI compreende a Direção de Tecnologias de Informação e Comunicações (DITIC)[39], que exerce funções enquanto órgão de direção técnica no domínio das TIC e das comunicações e sistemas de informação (CIS), sem prejuízo para as outras entidades que atuam no mesmo âmbito. Sendo a cibersegurança uma das suas áreas de responsabilidade, compete à DITIC:

> "Gerir, operar e manter a estrutura de segurança e defesa do ciberespaço e da informação na Marinha, assegurando a capacidade de resposta a incidentes no

[37] Ver Apêndice H – Entrevista ao Comandante Pratas Quaresma (COMNAV).
[38] Os OCAD, segundo o DR n.º 10/2015, de 31 de julho, têm como missão "assegurar a direção e execução de áreas ou atividades específicas essenciais", neste caso na gestão de recursos de informação.
[39] O organograma da DITIC encontra-se no anexo D.

> ciberespaço e de segurança da informação (CIRC) na Marinha, através de equipas próprias de combate às ameaças em computadores e em infraestruturas de redes (CERT ou CSIRT), disponibilizando processos e tecnologias que assegurem o adequado nível de segurança num contexto de gestão de risco" (DR n.º 10/2015 de 31 de julho).

Na sua estrutura, insere-se o Núcleo de Resposta a Incidentes de Segurança, também denominado Núcleo CIRC (*Computer Incident Response Capability*)[40], com a missão de garantir a segurança e a defesa do ciberespaço e da informação da Marinha. Foi através do NCIRC que a Marinha operacionalizou a CRISI.

Ao Núcleo compete ações de sensibilização para a comunidade utilizadora das redes e sistemas de Marinha, numa medida preventiva aos ciberincidentes, e a gestão e o tratamento dos mesmos. Neste sentido, o Núcleo monitoriza uma plataforma que deteta e regista todos os incidentes, em tempo real, que ocorrem nas redes de Marinha.

A CRISI foi operacionalizada também, no ano de 2012, a nível das UEO, com a criação dos cargos de Administrador do Domínio do Utilizador[41] (ADU), de Oficial de Segurança do Domínio do Utilizador (OSDU) e de Gestor Operacional do Domínio do Utilizador (GODU), em acumulação.

Estas três entidades concorrem igualmente, de forma relevante, para a organização da segurança das redes e sistemas de informação, com funções na operação, administração e segurança dos SICA (EMA, 2005). No entanto, o OSDU e o ADU são as entidades a quem compete especialmente a prevenção e a deteção dos ciberincidentes que possam ocorrer na respetiva UEO e, após a identificação de um incidente, responder e/ou recuperar do mesmo (EMA, 2012).-O ADU e o OSDU são a ponte entre a comunidade utilizadora das redes e sistemas da Marinha e o NCIRC.

Devido à permanente monitorização das redes de Marinha, é o NCIRC que tem capacidade para identificar no momento de ocorrência os incidentes nas UEO. Na eventualidade de a própria máquina protegida com o *software* não ser capaz de eliminar ou conter o incidente, o NCIRC notifica os respetivos ADU e OSDU da situação.

[40] O artigo que regula o NCIRC encontra-se em Anexo E.

[41] Pelo PCA 2, o domínio do utilizador "compreende o conjunto de recursos que permite a uma comunidade específica de utilizadores interligar-se ao domínio de rede, sob gestão e administração locais". Por sua vez, o domínio da rede "compreende todos os suportes e recursos de comunicações de âmbito alargado mas controlados e geridos de um modo centralizado, que viabilizam a transferência da informação ou dados entre domínios do utilizador".

Contudo, só intervém na resolução do incidente, caso estas entidades não sejam capazes de responder ao mesmo.

Assim, pode-se afirmar que a Marinha possui edificada uma organização para a segurança do ciberespaço. Neste domínio, é relevante que a sua estrutura seja contruída de acordo com a capacidade que pretende alcançar, "com autonomia em todos os setores e capaz de colaborar e cooperar com órgãos externos à Marinha" (Prates, 2019).

Operacionalmente, deverá ainda assegurar flexibilidade na sua estrutura para a construção de diferentes equipas, permitindo-lhe responder eficientemente aos objetivos propostos, incluindo os de C2 (Carvalho, 2019; Prates, 2019). Ainda a este nível, o COMNAV, responsável pela condução de operações, possui uma capacidade unicamente defensiva e muito pouco desenvolvida.

3.3. Treino

O Treino é a dimensão que visa preparar os "diferentes intervenientes para uma resposta pronta e capaz às necessidades" (Neves, 2015), sendo considerada como "essencial (…) para a manutenção e desenvolvimento de uma capacidade" (Neves & Correia, 2016). Assim sendo, o Treino, para cumprir com o seu objetivo de manter e desenvolver, deverá ser composto pela formação dos indivíduos, educação e sensibilização para o assunto e a realização de exercícios. Contudo, ao nível da educação e sensibilização será melhor tratado no subcapítulo *Pessoal*.

Segundo a NATO, deve ser assegurado tanto treino individual com foco nas competências individuais necessárias à execução de tarefas específicas, como treino coletivo para aplicação prática dessas mesmas competências e ser possível desenvolver o conhecimento adquirido (NATO, 2018c).

A realização de exercícios permite testar este conhecimento e retirar lições aprendidas com o propósito de obter uma capacidade mais eficaz e eficiente. Estas lições poderão ainda ser úteis no melhoramento e desenvolvimento de doutrina.

Conhecendo os riscos que acompanham o ciberespaço e a influência que qualquer utilizador de uma rede ou sistema de informação de Marinha poderá ter no seu ciberespaço, poderá considerar-se dois tipos de atuação. Nos que desempenham funções a nível técnico e operacional para a segurança do ciberespaço da Marinha e na comunidade de utilizadores dos SI e das TIC da organização.

O PCA 2 estabelece que todo o pessoal deve receber competências ao nível da "segurança informática", abordando os perigos, os meios de combate e a organização para a segurança. Devem ainda ser dotados de competências no uso do "computador e todas as ferramentas de escritório eletrónico" (EMA, 2005).

Embora a educação e a sensibilização componham duas áreas comuns a estes dois grupos, terão um papel mais crucial e notório no segundo. Pois os primeiros, por possuírem formação na área já deverão estar mais alertados para os riscos e as medidas de segurança a ter para os evitar.

Estes indivíduos requerem um conhecimento mais técnico conducente de determinado grau de qualificação para o cargo em específico. Como tal, deverão receber uma formação sólida na área. A existência de um treino adequado permite-lhes testar e desenvolver a suas competências, inclusivamente com outras entidades para a resposta a ciberincidentes.

Por proposta do Coordenador do NCIRC, os seus recursos humanos poderão receber formação através de duas vias, pelo Plano de Anual de Formação de Marinha (PAFM) ou por cursos propostos pelo CCD aos três ramos. O CCD possui como competência no âmbito da ciberdefesa, "contribuir para o plano de formação, treino e qualificação dos recursos humanos das Forças Armadas" (DR n.º 13/2015 de 31 de julho).

Há que ter em atenção que o ciberespaço constitui-se como um espaço dinâmico e complexo, onde os seus perigos intensificam-se a um ritmo preocupante. Neste sentido, a formação da chefia e das suas equipas deverá ser contínua, de modo a estarem preparados e aptos a responder prontamente aos incidentes que ocorram nas redes e sistemas de informação da Marinha.

A comunidade de utilizadores pode comprometer a segurança do ciberespaço da organização e deve por essa razão, ser educada e sensibilizada para o tema. Internamente, cabe ao NCIRC alertar e consciencializar a comunidade de gestores e utilizadores dos sistemas de informação.

Desta forma, é responsável por controlar conteúdos, elaborar recomendações de segurança e publicar alertas e boletins informativos (*Regulamento Interno da DITIC*, 2016). Através da sua página CRISI, na Intranet de Marinha, são disponibilizadas muitas destas informações, incluindo ainda notícias relevantes, documentos que possam ser necessários, como legislação interna e internacional, e ainda relatórios e documentos relativos a exercícios cibernéticos onde a Marinha participa.

O Núcleo é ainda responsável pela realização de palestras com a finalidade de sensibilizar os utilizadores para os riscos do ciberespaço e para a adoção de boas práticas neste âmbito.

O GT-EMA assume como imprescindível que tanto os utilizadores, como a chefia de topo, sejam sensibilizados de que a ciberdefesa é uma questão inerente a qualquer indivíduo e desse modo, deva ser uma preocupação de todos. A atualização dos conhecimentos para uma abordagem mais pronta aos riscos do ciberespaço deverá também ocorrer a este nível. Neste sentido, a Marinha providencia por vários intervenientes, formações base à sua comunidade.

Para além das ações já mencionadas, o NCIRC preparou um curso básico denominado de *Conceitos Gerais de Cibersegurança* e que é ministrado pela Escola de Tecnologias Navais (ETNA)[42]. Este curso é apresentado no Curso de Formação de Praças (CFP) a todas as praças de Marinha.

Nos mesmos moldes, é ainda facultado o curso AKS70 a todo o universo de Marinha (civis, militarizados, praças, sargentos e oficiais). É um curso de aperfeiçoamento de conceitos gerais de cibersegurança, distinguindo-se por acrescentar no seu currículo a doutrina de Marinha para a conceção e operação de sistemas de informação.

Esta escola possui ainda como apoio à sua oferta formativa uma academia Microsoft onde são fornecidos conteúdos e momentos de avaliação dos seus alunos, a qual se prevê que seja brevemente acessível a todo o pessoal da marinha. A ETNA pretende ainda a curto/médio prazo disponibilizar o curso de formação para OSDU, ADU e GODU, entidades com funções desde 2012 e que desde então, nunca receberam formação para tal. Esta ação foi proposta pelo NCIRC, mas ainda se encontra em aprovação (Alexandre, 2019a)[43]. O Curso de Formação de Sargentos (CFS) prevê também a adoção de um módulo em cibersegurança.

A ETNA, através do seu Gabinete de Sistemas de Informação (GSI), é responsável por sugerir e implementar estes cursos, cooperando com o NCIRC. Embora a sua oferta formativa se encontre a crescer, é ainda muito básica. O seu maior impedimento revela-se pela falta de pessoal qualificado, ocupado muitas vezes em "assegurar a formação prevista ou a atualizar os seus conteúdos" e que dessa forma tem menos disponibilidade

[42] A ETNA é uma escola que tem como principal missão fornecer formação técnico-profissional aos militares da Marinha, principalmente a sargentos e praças, contribuindo ainda para a formação técnico-naval dos seus oficiais.
[43] Informação confirmada em entrevista presencial com o atual Coordenador do Núcleo, Comandante Courela Alexandre, em 20-03-2019.

para "investigação e desenvolvimento (pelo menos sem apoio externo) de novos cursos" (Veloso, 2019)[44].

A Escola Naval (EN), que visa a formação dos futuros oficiais da Marinha, ministra atualmente um curso de *e-learning* e que fornece os conhecimentos básicos de cibersegurança para todos os cadetes de 1.º ano.

Em parceria com o Instituto Superior Técnico e a Faculdade de Direito de Lisboa, a EN disponibiliza um mestrado em "Segurança da Informação e Direito do Ciberespaço". Da mesma forma, também a Academia Militar ministra um mestrado, por sua vez em "Guerra da Informação".

A nível geral das FFAA, além da atuação do CCD, o Instituto Universitário Militar (IUM) também contribui para a formação do universo militar ao facultar o Curso de Planeamento de Operações De Ciberdefesa (CPOCIBER)[45] e para a consciencialização dos utilizadores através de seminários e palestras (IUM, n.d.).

A NATO compreende ainda um projeto liderado por Portugal, denominado por *Multinational Cyber Defense Education and Training* (MN CD E&T) e no qual a Marinha participa. Este projeto concorre para a formação do pessoal e simultaneamente para interoperabilidade no âmbito da ciberdefesa.

O MN CD E&T tem como objetivo criar uma plataforma que coordene uma rede de atividades de educação e treino e possibilite novas iniciativas que respondam a este tipo de necessidades na NATO e nas suas nações aliadas (Exército Português, n.d.). Mais concretamente, visa a identificação e a preparação das competências adequadas às funções desempenhadas pelos utilizadores.

Deste projeto surge a iniciativa *Cyber Academia and Innovation Hub* lecionada na Academia Militar até entrar em funcionamento a NCI *Academy,* em Oeiras. O seu objetivo é formar os participantes nas áreas da cibersegurança e da ciberdefesa (VdA Academia, 2018). Estes projetos possibilitam oportunidades de formação à Marinha e restante universo de operadores nas FFA. A NCI *Academy* irá ministrar cursos de *e-learning* e certificar as diversas competências exigidas.

Relativamente à realização de exercícios, a Marinha envolve as suas equipas em exercícios internos, nacionais e internacionais, muitos deles já referidos no capítulo

[44] Ver Apêndice G - Entrevista ao Tenente Castro Veloso (ETNA).
[45] O CPOCIBER é um curso de especialização que fornece formação teórica e técnica necessária ao desempenho de tarefas no âmbito das operações no ciberespaço, em funções de Estado-Maior de forças nacionais e internacionais.

anterior. As suas equipas, a nível dos exercícios externos, são constituídas por elementos com formação técnica em ciberdefesa e por elementos da área jurídica que dão pareceres relativamente às várias ações neste âmbito. Os exercícios compõem uma das linhas de ação da ENSC 2.0, relacionando-se com o domínio da Interoperabilidade, visando "[reforçar e aumentar] o nível de maturidade para a proteção do ciberespaço" (RCM n.º 92/2019 de 5 de junho).

Nos exercícios nacionais navais INSTREX, CONTEX/PHIBEX e SWORDFISH são conduzidas séries ao nível da ciberdefesa. Quem assume a coordenação destas séries de ciber é a DITIC, através do NCIRC, mas em estreita coordenação com o COMNAV. Estas séries consistem em exercícios consideravelmente acessíveis e a ser resolvidos pelo ADU com o auxílio do GODU. Neste sentido, o EMA confirma a necessidade de um maior empenho na preparação e realização de séries deste âmbito em exercícios nacionais, aumentando o seu número e a sua complexidade (GT-EMA, 2018).

No treino externo, a Marinha participa nos exercícios nacionais Ciber Perseu, anualmente organizado pelo Exército e mais virado para o treino de ciberdefesa das Forças Armadas, e Lusitano, um exercício conjunto com os ramos e o EMGFA.

Em exercícios internacionais e alguns nacionais, a Marinha participa através da atribuição de alguns dos seus elementos qualificados na área, sob a coordenação e direção do CCD. Assim, por este órgão, participa nos seguintes exercícios internacionais NATO, o *Cyber Coalition*, o *Locked Shields*, o CMX (*Crisis Management Exercise*) e o CWIX (*Coalition Warrior Interoperability Exercise*). Ainda a nível internacional, participa no IberoAmericano de Ciberdefesa e no *Cyber Europe* da ENISA. Já os exercícios nacionais, compreendem o CyberDEx e o ExNCS.

O treino existente na Marinha foca-se essencialmente nos indivíduos e órgãos que desempenham funções na segurança das redes e dos sistemas de informação. Contudo, como já discutido anteriormente sobre a relevância que a comunidade utilizadora tem neste âmbito, pode-se questionar se não será também útil promover algum tipo de treino adequado à Marinha no geral. Estas ações iriam preparar melhor a comunidade na utilização das redes e sistemas e contribuir bastante para a prevenção de incidentes cibernéticos.

Ainda assim, atualmente a Marinha tem integrado diversos exercícios, tanto a nível nacional como internacional, que permitem promover a formação dos seus recursos humanos, sendo um fator fulcral para a edificação da sua capacidade de ciberdefesa.

3.4. Material

A dimensão do material compreende todos os meios necessários que permitam equipar, manter e suportar os indivíduos e as equipas nas suas atividades (NATO, 2018a). Ainda da mesma definição decorre que estes meios excluem os imóveis, as instalações e os utilizadores, incluídos nas restantes dimensões apresentadas ao longo do capítulo.

Para o presente tema, no Material inserem-se todos os meios adequados às necessidades dos utilizadores, operadores e líderes que permitem manter e assegurar a segurança das redes e dos sistemas de informação. Este material inclui "os equipamentos, a tecnologia, as infraestruturas de comunicações", entre outros, "ou seja, todo o material que tenha relevância para o sucesso da missão" (Neves, 2015).

Os requisitos técnicos e de segurança dos materiais diferem com a finalidade dos mesmos. Para qualquer SICA da Marinha, as medidas de segurança devem garantir a "confidencialidade, integridade, e disponibilidade de si próprio e da informação em si processada, armazenada e transportada" (EMA, 2005).

Para a informação classificada ou sensível[46], esta deve adotar as "medidas de segurança compatíveis com o grau de classificação de segurança das matérias ou o valor das mesmas, e ainda a especificidade das tecnologias utilizadas", independentemente do material físico que a suporta (EMA, 2005). Pela mesma fonte, deve ainda ser assegurado a devida "proteção contra "ataques informáticos", através do emprego de soluções, políticas e procedimentos de segurança".

Para a missão do NCIRC é essencial possuir os sistemas, equipamentos e tecnologias necessários e adequados que lhe permitam detetar, analisar e recuperar dos incidentes de segurança da informação, como as plataformas de monitorização de eventos e de registo dos mesmo, ou os meios de comunicação com entidades internas e externas (EMA, 2012; Neves, 2015). Além de serem possuidores destes materiais, para o cumprimento eficaz das suas funções, devem cumprir com os requisitos de segurança já mencionados.

No mesmo sentido, o material utilizado pela comunidade de utilizadores da Marinha deve também apresentar os requisitos mínimos de segurança, pois como utilizadores

[46] O conceito de informação sensível define-se como a "informação que, por decisão de uma autoridade competente, deve ser protegida porque a sua divulgação, modificação, destruição ou perda pode provocar graves prejuízos a bens ou a pessoas" (EMA, 2006).

finais da rede, poderão comprometê-la. Este material inclui o *hardware*, o *software* do sistema e os *softwares* aplicativos[47], entre outros.

De modo a evitar a ocorrência de incidentes a níveis mais significativos, os SICA devem garantir a existência de perfis de utilizadores de acordo com o princípio da "necessidade de conhecer", limitando a visualização e o manuseio da informação e dos dados e evitando expô-la sem necessidade (EMA, 2005).

Estas medidas, entre outras, estão definidas no SEGNAC 4. Este documento apresenta uma série de normas que visam garantir a segurança dos sistemas informáticos. Neste campo, o GNS é a autoridade nacional de credenciação no acesso e manuseio de informação classificada, sendo que deve "avaliar, acreditar e certificar a segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada e proceder à realização de limpezas eletrónicas" (DL n.º 3/2012 de 16 de janeiro). Compete ainda ao GNS assegurar que o material criptográfico é alvo das necessárias medidas de segurança.

Todo o material utilizado com implicações na segurança das redes e dos sistemas de informação deve cumprir com os requisitos de gestão de risco. O cumprimento destes requisitos, tanto nas aquisições a realizar, como na cadeia de abastecimento, foram referenciados na ENSC 1.0 como uma das atividades já realizadas pelo EMGFA em 2015 e constituindo-se como uma das medidas para o desenvolvimento da capacidade de ciberdefesa.

Segundo o GT-CCFA, muitos dos seus sistemas operacionais necessitam de ser atualizados ou mesmo substituídos. Pois só assim, são capazes de garantir a proteção dos sistemas e redes de informação das FFAA. A sua deficiente defesa torna os seus sistemas suscetíveis às ameaças do ciberespaço e a sua interligação às restantes redes e sistemas propaga esta ameaça, comprometendo o seu correto funcionamento e a segurança da sua informação.

Pode-se considerar que a Marinha contém o material necessário para garantir o suporte e prover as equipas para o desempenho das suas funções, contudo é essencial que se mantenham os sistemas atualizados e com elevados níveis de desempenho (Neves,

[47] O *hardware* refere-se a todas as peças internas (e.g. processador) e externas (e.g. *pendrive*) que compõem os computadores. O *software* do sistema são todos os programas que vêm incluídos no sistema operacional do computador, tal como as ferramentas do sistema e a limpeza do disco. Já o software de aplicação, consiste nos programas adicionados pelo utilizador, tal como o antivírus ou o Word.

2019). Sendo assim, por recomendação do GT-CCFA, esta deve ser uma área de investimento para evitar operar sistemas obsoletos que possuam reconhecidas vulnerabilidades e deficiências ao nível da segurança.

Desta forma, a Marinha deve não só possibilitar os bens materiais necessários à capacidade de segurança do ciberespaço do seu interesse, como garantir que esses meios cumpram com os requisitos de funcionamento e segurança, por forma a não facilitar e impedir o comprometimento das suas redes e sistemas, bem como da informação neles contida.

3.5. Liderança

A Liderança é uma das vertentes associadas aos recursos humanos e consiste no "desenvolvimento profissional de líderes para produzir os indivíduos mais competentes possíveis" (NATO, 2018a).

É essencial que o líder tenha uma preparação técnica adequada ao exercício do respetivo cargo, de modo a comandar, dirigir e motivar a equipa, "sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão" (Neves & Correia, 2016).

Nas suas competências, um líder deve assegurar que a equipa possui "uma visão partilhada do propósito e objetivos" da missão, encorajar ao seu esforço e trabalho em equipa em prol de uma maior eficácia coletiva, atender à resolução de conflitos e asseverar a sua coordenação (Santos, Caetano, & Jesuíno, 2008). Segundo a mesma fonte, "a liderança é um importante fator que pode afetar os processos de equipa e os seus resultados". Revelando assim, um grande impacto na eficácia e eficiência de uma tarefa ou missão.

Na vertente da Liderança e para a ciberdefesa, não são unicamente os líderes das equipas que desempenham funções na área da segurança e defesa do ciberespaço que se incluem neste subcapítulo, mas também os líderes das UEO, pelo impacto que a comunidade utilizadora pode ter na segurança cibernética da Marinha.

Contudo, as competências atribuídas anteriormente na resolução de tarefas, são mais específicas para o primeiro caso. E neste sentido, "ainda existe um importante caminho a percorrer" (Neves, 2019), revelando-se uma falta de preparação para assumir cargos neste âmbito, tópico que será abordado no subcapítulo *Pessoal*. No entanto, indica-se como

uma das soluções a "participação das chefias em *fóruns* dedicados, com especial foque na estratégia e nos efeitos" (Prates, 2019).

No segundo caso, os líderes devem ter consciência das consequências que os perigos cibernéticos podem ter para os próprios serviços e especialmente para a Marinha no geral, assumindo a relevância de os prevenir e assegurar a segurança das suas redes e sistemas. Esta perceção não deve ficar só pelo líder, ou seja, este elemento deve assegurar a sensibilização sobre o atual paradigma do ciberespaço às suas equipas. Segundo o GT-EMA, atualmente as chefias não estão sensibilizadas sobre a relevância da ciberdefesa para a organização e as consequências que um ataque deste tipo pode causar à Marinha.

Desta forma, o GT-EMA revela a necessidade de tornar as chefias conscientes sobre este tema e não apenas os departamentos técnicos na área das tecnologias de informação. Assume-se assim, que a vertente da Liderança na edificação da capacidade de ciberdefesa na Marinha, deverá ser considerada de forma transversal a toda a organização.

3.6. Pessoal

Este domínio refere-se aos recursos humanos, sejam militares, militarizados ou civis, necessários ao cumprimento de uma missão ou tarefa (NATO, 2018a). Os indivíduos da organização devem possuir as qualificações necessárias ao desempenho das suas funções. Contudo, como já referido anteriormente, pelas características do ciberespaço, a comunidade de utilizadores das redes e sistemas de informação tem uma grande influência na garantia da sua segurança. Assim sendo, este último deverá também consistir numa área de atuação.

Ao nível técnico, a Marinha possui o NCIRC, constituído por Analistas Forenses, Gestores de Incidentes e Monitores de Incidentes, correspondente a três níveis de capacidade técnica diferentes[48], do mais alto para o mais baixo respetivamente, e o qual é chefiado pelo Coordenador do Núcleo. Este último elemento deverá não só possuir as competências técnicas de acordo com o trabalho realizado no Núcleo, como também as competências de liderança referidas no subcapítulo anterior.

Ao Coordenador do Núcleo compete gerir diariamente o Núcleo, garantindo o seu normal funcionamento. Este elemento é responsável por planear as diversas atividades que envolvem o NCIRC, como exercícios de treino, ações de sensibilização e ações de

[48] Os níveis técnicos necessários para o desempenho de funções são de acordo com o Quadro Nacional de Qualificações, regulado pela Portaria n.º 782/2009 de 23 de julho.

formação para a sua equipa, de acordo com as funções exercidas pelos seus elementos (*Regulamento Interno da DITIC*, 2016).

É através do Coordenador do Núcleo, representante do mesmo, que é realizado o contacto com outras entidades, tanto a nível interno de Coordenação, como externo à Marinha, neste último caso, com o CCD. O cargo de Coordenador é assegurado, em acumulação, por um oficial superior que chefia simultaneamente o Gabinete de Projetos, Normalização e Segurança (GPNS).

Num paradigma onde a cibersegurança assume um papel tão determinante no desempenho de qualquer organização e neste caso, para a Marinha, questiona-se se a chefia do núcleo não deveria ser vista como prioritária e o seu cargo assumido em lotação. Enquanto chefe de uma equipa técnica, este oficial deveria também receber uma formação prévia e adequada para o exercício das suas funções. Segundo o testemunho do atual Coordenador do NCIRC, até ao momento de assumir o cargo e após os primeiros meses de exercício de funções, não recebeu formação específica para tal (Alexandre, 2019a).

O cargo de Analista Forense é preenchido por oficiais subalternes com uma forte formação técnica. Tal como o Coordenador do Núcleo, os Analistas também acumulam funções, o que impossibilita a completa disponibilização dos mesmos para executarem todas as tarefas incumbidas (GT-EMA, 2018; Neves, 2015; Alexandre, 2019a). A sua formação é contínua e proposta superiormente e anualmente pelo Coordenador do Núcleo.

Os Analistas Forenses são responsáveis por investigar os incidentes quando existe a necessidade de aplicar um conhecimento técnico mais elevado, bem como apoiar o Coordenador do Núcleo no planeamento de atividades. Quando a criticidade do incidente de segurança exige uma capacidade de investigação superior, o Coordenador do Núcleo toma conhecimento e torna-se responsável por definir as ações seguintes de forma a solucionar o incidente. Neste sentido, através do Coordenador e como já referido anteriormente poderá ser solicitada a cooperação com entidades externas à Marinha (Neves, 2015; Alexandre, 2019a).

Os Gestores de Incidentes são procedentes do quadro de sargentos e equivalem a um nível técnico intermédio. É a estes elementos que compete a primeira triagem dos eventos[49] cibernéticos. Após a triagem, os Gestores de Incidentes podem validá-lo como

[49] Pelo PCA 16, um evento é "qualquer ocorrência observável que pode ocasionar um incidente de segurança da informação", o que por sua vez, este último conceito, é definido como "uma ação ou

não incidente e fechar o caso, ou numa situação contrária, fazer a investigação do incidente e dependendo da exigência da sua resolução e tratamento, requerer o auxílio dos Analistas Forenses (GT-EMA, 2018; Neves, 2015; Alexandre, 2019a).

Os Monitores de Incidentes são elementos do quadro de praças e com um nível técnico menos exigente. Os Monitores de Incidentes monitorizam as plataformas de controlo e gestão de eventos do Núcleo, a partir das quais são detetados todos os eventos e incidentes, procedendo-se ao registo de todos os incidentes que necessitem de ser tratados pelos Gestores de Incidentes.

Os cargos inseridos na estrutura definida para o Núcleo, não se encontram totalmente preenchidos, adicionando já à questão da acumulação interna de funções. A existência destas situações origina a "sobrecarga das tarefas para os elementos do Núcleo". Ainda assim, pode-se considerar que o NCIRC tem sido capaz de "cumprir satisfatoriamente a sua missão" (Neves, 2019).

Ao nível das UEO, tal como referido no subcapítulo da Organização, existem três entidades, o OSDU, o ADU e o GODU. Pelo PCA 2, o OSDU é "responsável pelo cumprimento das normas e procedimentos de segurança (POpS) aplicáveis aos serviços existentes no seu domínio" e ao ODU compete o "controlo de configuração de todos os serviços disponibilizados no seu domínio e pela implementação das normas e procedimentos de segurança comuns a esses serviços" (EMA, 2005). O GODU é a entidade "responsável pela operação de todos os serviços disponibilizados no seu domínio [e representa] a comunidade de utilizadores dos diversos sistemas existentes no seu domínio" (EMA, 2005).

A nomeação destes cargos é determinada pelo Comandante, Diretor ou Chefe mais antigo de cada UEO e ao qual está associado um Domínio de Utilizador que permite à respetiva comunidade de utilizadores o acesso a diferentes tipos de serviços (EMA, 2005).

Embora estes cargos tenham sido criados em 2012, desde então não foi definida nenhuma ação de formação destinada a preparar melhor estes elementos. Admite-se, portanto, que os ADU e os OSDU têm "uma enorme falta de formação técnica" (Neves, 2019) e que necessitam de formação e experiência para adquirir as perícias adequadas para o desempenho eficaz dos respetivos cargos (GT-EMA, 2018).

conjunto de ações desenvolvidas num ou mais SICA que resulta, ou pode resultar, na perda da confidencialidade, integridade e/ou disponibilidade da informação" (EMA, 2012).

Atualmente, como apoio às suas funções, o NCIRC disponibiliza, na Intranet de Marinha, um conjunto de cinco documentos que descrevem procedimentos a ser tomados pelo ADU e que permitem identificar e tratar alguns dos incidentes cibernéticos mais comuns nas UEO.

A componente dos recursos humanos é um dos fatores mais críticos no desenvolvimento da capacidade de ciberdefesa, apontando-se vários fatores neste sentido, discutidos de seguida. Contudo, a sua criticidade pode ser vista de dois lados. Pela perigosidade que qualquer utilizador pode causar na segurança das redes e sistemas ou pelos recursos humanos associados ao domínio técnico e operacional necessários a garantir a segurança do ciberespaço e a resposta a incidentes.

O GT-EMA assume como uma das medidas mais eficaz face ao ciberataques, a formação e consciencialização de todos os indivíduos pertencentes à Marinha, referindo ainda que o Homem é responsável por 95% dos comprometimentos dos sistemas, especialmente devido à carência de boas práticas[50]. Desta forma, torna-se conveniente e prioritário garantir formações base a todos os utilizadores das redes e sistemas de Marinha.

Já no segundo caso, a qualificação dos técnicos e operadores, o seu recrutamento e a permanência nas suas funções são fatores que dificultam o desenvolvimento da ciberdefesa na Marinha. Neste sentido, são apontados como obstáculos a "dificuldade de identificação dos ativos humanos", a deficiente formação e a dificuldade em "atrair novos elementos para os quadros" na área da ciberdefesa (Neves, 2019). Este último ponto deve-se principalmente à alta valorização, dos elementos que possuem estas competências, no mercado de trabalho.

Esta formação é "complexa, dispendiosa e leva muito tempo" (Jesus, 2019). Sendo de destacar novamente que devido ao tema em questão, os conhecimentos do pessoal especialmente técnico e operador, deve ser mantido em constante atualização. O ciclo de formação deste pessoal tem um período de cerca de um a dois anos.

A curta permanência em cada cargo e a disparidade das funções, como é comum nas FFAA, entre dois a três anos, são fatores que não abonam a favor do tempo e orçamento despendido nos recursos humanos.

[50] O EMA remete este facto para a seguinte fonte: Palestra do CNCS, no 5º Curso Geral de Cibersegurança, em setembro de 2017, sobre os comprometimentos.

Neste sentido, o EMGFA, para preenchimento dos cargos existentes no CCD e rentabilização da formação e treino destes militares, implementou, após solicitação aos próprios ramos das FFAA, e pelo definido na ENSC 1.0, a permanência dos seus efetivos nos cargos num mínimo de cinco anos. A mesma fonte destaca que a mesma medida deve estender-se a todas as funções técnicas relativa à vertente da ciberdefesa.

A falta de recursos qualificada é verificada a "vários níveis, operacional, tático e estratégico, [comprometendo] a sustentabilidade da capacidade a médio prazo" (Neves, 2019). A "escassez de recursos humanos" obriga à acumulação de cargos e funções, sobrecarregando-os e impossibilitando-os "de executar corretamente todas as tarefas que lhe estão atribuídas" (Neves, 2019). Além da sua captação, a "retenção e identificação de elementos capazes e consequentemente adaptação orgânica" (Prates, 2019) são pontos-chave para a capacidade de ciberdefesa.

Neste domínio, a ENSC 2.0 apresenta diversas linhas de ação que, embora não se encontrem definidas especificamente para as FFAA, são vantajosas e aplicáveis aos seus ramos. São elas a promoção de programas que capacitem as organizações para a adoção de bons hábitos e a consciencialização da responsabilidade individual para a cibersegurança; a criação de "mecanismos de retenção em entidades nacionais de recursos qualificados" e o aproveitamento das "estruturas de ensino e formação militares (…) nacionais e internacionais" (RCM n.º 92/2019 de 5 de junho).

A vertente do Pessoal, tanto ao nível dos técnicos como da comunidade, é apresentada por todos os entrevistados como fundamental para a capacitação da Marinha na segurança do ciberespaço e uma das principais lacunas que a organização apresenta na sua capacidade de ciberdefesa. Esta criticidade é comum a nível nacional, apresentado na ENSC 2.0 como uma vulnerabilidade.

3.7. Infraestruturas

A dimensão das Infraestruturas consiste nas instalações compostas por "um edifício, estrutura, sistema de utilidade, pavimento e/ou terreno subjacente" (NATO, 2018a). Para as Infraestruturas e considerando a capacidade que se pretende atingir, não são muito exigentes as que se requerem, mesmo para o nível mais técnico deste organização (Neves & Correia, 2016).

Aponta-se como relevante a segurança física das instalações, onde devem ser implementadas medidas de segurança nas áreas onde "existam SICA que processem

informação classificada ou sensível, devendo o pessoal com acesso autorizado, possuir a adequada credenciação e necessidade de conhecer" (EMA, 2005). Embora este fator seja dos mais importantes, não se deve excluir as condições de habitabilidade em que as equipas deverão executar as suas funções.

A segurança física das instalações é definida nos SEGNAC 1, 2 e 4. As áreas que contêm equipamentos informáticos e seus relativos devem cumprir com a classificação das áreas de segurança estabelecidas nos dois primeiros SEGNAC. No último são estabelecidas normas de segurança para os centros de informática. Estas normas visam "garantir a segurança dos dados, programas e materiais classificados contra a espionagem, sabotagem, terrorismo, comprometimento e divulgação não autorizada, especialmente captação de radiações eletromagnéticas, introdução (…) [de] "vírus informáticos" e violação dos acessos lógicos" (RCM n.º 5/90 de 28 de fevereiro).

O SEGNAC 4 define ainda as características das áreas compostas por estes equipamentos. O nível de proteção física deve ser aplicado consoante determinados fatores, mais concretamente com o grau de classificação das matérias a proteger, com os equipamentos a salvaguardar, com a credenciação e necessidade de conhecer do pessoal e, por fim, com as ameaças derivadas de atividades terroristas ou criminosa (RCM n.º 5/90 de 28 de fevereiro).

Este documento é maioritariamente aplicável ao NCIRC por ser o órgão técnico na Marinha com responsabilidade na resposta a incidentes da segurança da informação e deve apresentar uma maior resiliência em situações de crise[51]. As suas instalações devem cumprir com requisitos ao nível da localização e estrutura, energia elétrica, climatização, proteção contra incêndios e radiações eletromagnéticas e controlo de acesso do pessoal.

Embora todos estes fatores sejam relevantes, destaca-se a proteção elétrica das instalações. Pelas características dos serviços retratados a nível tecnológico, a energia elétrica torna-se um suporte indispensável aos mesmos. Especialmente para o NCIRC, este deve assegurar a continuidade dos seus serviços para prevenção e defesa das redes e sistemas de Marinha através de "sistemas de segurança adicionais, tais como geradores de corrente elétrica e sistemas no-break" (RCM n.º 5/90 de 28 de fevereiro).

No presente domínio, é possível afirmar que as infraestruturas existentes são adequadas às necessidades, não se destacando como uma preocupação segundo os

[51] Pelo PCA 16, crise é uma "situação que decorre de um ou mais incidentes de segurança da informação, que afeta gravemente o desempenho da organização, assim como os seus recursos" (EMA, 2012).

entrevistados, devendo, no entanto, ser assegurada "a sua sustentabilidade e manutenção" (Neves, 2019).

3.8. Interoperabilidade

A Interoperabilidade é o domínio que consiste na "capacidade de atuar em conjunto de forma coerente, eficaz e eficiente para alcançar os objetivos táticos, operacionais e estratégicos" da organização (NATO, 2018a). A operação conjunta das diferentes entidades é possível através da harmonização de "padrões, doutrinas, procedimentos e equipamentos" (NATO, 2017b). Segundo o GT-CCFA, a interoperabilidade é uma condição indispensável a alcançar tanto no contexto nacional como internacional.

No âmbito da ciberdefesa, a Marinha colabora com várias entidades, direta e indiretamente, tanto a nível nacional como internacional. O estabelecimento destas relações deve-se a diferentes órgãos empenhados numa organização estrutural com o fim de garantir a segurança do ciberespaço de interesse dos vários atores, através de um esforço colaborativo e essencialmente, de partilha de informação.

Compete ao NCIRC da Marinha, diversas ações que asseguram o desenvolvimento do domínio da Interoperabilidade. Delas fazem parte a colaboração com o CCD e com os NCIRC dos ramos militares para responder a ciberincidentes nas FFAA ou ao nível das infraestruturas críticas nacionais; colaborar com os restantes Núcleos CIRC que participam na capacidade de ciberdefesa nacional; participar em exercícios nacionais e internacionais neste âmbito; e partilhar informação com os Núcleos CIRC nacionais e internacionais (*Regulamento Interno da DITIC*, 2016).

Pelo GT-CCFA é constatado que cada NCIRC dos ramos não apresenta uma estrutura comum para a resposta a incidentes, pela sua orgânica singular e orientada para a especificidade do respetivo ramo. Desta forma, ao não estarem harmonizadas questiona-se a sua capacidade de interoperabilidade face à resolução de incidentes ou a uma crise cibernética.

O NCIRC da Marinha colabora diretamente com o CCD e é a partir deste órgão que se asseguram as restantes ligações às entidades externas, estabelecendo-se de acordo com o apresentado na figura 2. Entre as entidades militares, como o NATO NCIRC e o CCD, e as entidades civis, como a ENISA e o CNCS, existe uma estreita colaboração.

Figura 2 Relações de Interoperabilidade

Fonte: Alexandre, 2019

O CCD é o órgão responsável por dirigir e coordenar a capacidade nacional de ciberdefesa, sendo a autoridade técnica no âmbito da ciberdefesa e da cibersegurança setorial da defesa nacional. Ao CCD compete "garantir a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas" [52] (DR n.º 13/2015, de 31 de julho).

No âmbito da ciberdefesa, é responsável por coordenar e assegurar a colaboração dos NCIRC, colaborar com o CNCS e os vários CIRC nacionais e internacionais, através da partilha de informação, e propor a participação dos órgãos com capacidade de ciberdefesa nos organismos nacionais e internacionais.

Na cibersegurança setorial da defesa nacional, compete ainda ao CCD coordenar e assegurar a colaboração dos CIRC do universo da defesa nacional e cooperar com as entidades nacionais que são responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo. Com a coordenação e pelo CNCS, o CCD colabora com os CIRC nacionais e internacionais com a partilha de informação.

Este último parágrafo cumpre com duas atividades referenciadas na Estratégia 1.0 como medidas necessárias ao desenvolvimento da capacidade de ciberdefesa. O estabelecimento de procedimentos de operação com a Polícia Judiciária (PJ) e o Serviço de Informações de Segurança (SIS) com a coordenação do CNCS e o desenvolvimento de um sistema de partilha de informação que ocorresse aos vários níveis e patamares de decisão, bem como para procedimento de alerta imediato, entre o CCD e os CIRC.

[52] Ver anexo A com as competências do CCD.

Pela ENSC em vigor, pretende-se desenvolver o "emprego dual das capacidades de ciberdefesa, no âmbito das operações militares e da cibersegurança nacional", através da partilha da informação (RCM n.º 92/2019 de 5 de junho). Ainda neste sentido, apresenta como linha de ação para "efeitos de gestão de crise", a participação coordenada das "Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas", para uma "abordagem integrada às ameaças e riscos" do ciberespaço (RCM n.º 92/2019 de 5 de junho).

Do exposto na ENSC 2.0, a interoperabilidade deve ainda ser assegurada através da "participação nacional nas diversas atividades de ciberdefesa no contexto internacional onde Portugal se insere", na participação de exercícios "onde a partilha de informação e conhecimento constitui um fator fundamental" e através da integração em organismos internacionais de ciberdefesa (RCM n.º 92/2019 de 5 de junho).

Como ferramentas para o desenvolvimento da interoperabilidade, Portugal utiliza uma plataforma de partilha de informação internacional sobre *malware*, o MISP (*Malware Information Sharing Platform*). A nível NATO, existem contribuições a que Portugal ainda não aderiu, como a ferramenta INSIGHT, para partilha de informação classificada relativa a incidentes cibernéticos e que corre na NATO *Secret Wide Area Network* (NSWAN). Já para a partilha de informação não classificada, a NATO utiliza o *Cyber Information and Incident Coordination System* (CIISS) e que também seria uma ferramenta prestável para a ciberdefesa na Marinha.

Ainda pela NATO, os projetos que Portugal integra e envolve a Marinha competem para o desenvolvimento da interoperabilidade. Para tal, como referido anteriormente, Portugal lidera o projeto MN CD E&T, em linha com o projeto *Smart Defence* da NATO e com a NATO CIA em Oeiras.

Para o alinhamento de conceitos e doutrinas num esforço nacional e particularmente militar, a Marinha serve-se de vários documentos partilhados pelas organizações a que pertence e nações aliadas e baseia-se neles no desenvolvimento de nova doutrina e para complemento da já existente.

A página da CRISI/NCIRC disponibiliza aos utilizadores da Intranet da Marinha uma série de documentação da UE e da NATO. O Núcleo para desempenho das suas funções também tem acesso a um portal da NATO para pessoal credenciado e que fornece vários documentos. Ainda neste sentido, o CCDCOE contém no seu *website* oficial, uma página dedicada à partilha de documentação no âmbito da ciberdefesa e com vários campos de aplicação.

Neste sentido, a Marinha participa atualmente em diversos campos que promovem a sua interoperabilidade num contexto nacional e internacional. Neste domínio, destaca-se a sua participação em exercícios, que permitem "assegurar a transversalidade de procedimentos, de equipamentos e de serviços no universo da defesa e demais órgãos com responsabilidades na segurança do ciberespaço" (Prates, 2019). É apresentada como crítica, a interoperabilidade que o ramo deve deter com o CCD, o CNCS e os aliados (Carvalho, 2019), revelando-se como um fator fulcral na edificação da sua capacidade de ciberdefesa.

Conclusões

O presente trabalho de investigação, tem como principal objetivo conhecer a capacidade que a Marinha Portuguesa tem no domínio da cibersegurança, reconhecendo as suas principais vulnerabilidades e a relevância do presente tema para a organização. De modo a cumprir com o mesmo, definiram-se certos objetivos secundários, expressos na *Introdução*, e os quais foram respondidos ao longo do desenvolvimento da dissertação.

A maioria dos serviços que competem para a ciberdefesa "baseiam-se funcionalmente nas capacidades técnicas, tradicionalmente associadas à cibersegurança" (Despacho 13692/2013 de 28 de outubro). Esta, expondo-se pelo "conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" (RCM n.º 92/2019 de 5 de junho), permite assegurar a capacidade de ciberdefesa que consiste em "assegurar a defesa nacional no ou através do ciberespaço". Deste modo, admite-se a cibersegurança como primeira linha da ciberdefesa.

Realça-se ainda que a cibersegurança é também ela garantida não só através dos processos que se baseiam a ciberdefesa, como pela articulação existente entre as diversas entidades externas que num esforço conjunto competem para a segurança do ciberespaço nacional, inserindo-se, no nível operacional, o CCD.

A capacidade de ciberdefesa da Marinha, no sentido do ponto acima referido, pode ser edificada/desenvolvida numa abordagem DOTMLPI-I e com a conjugação de todos os seus domínios. Neste sentido, foi levantada a capacidade que este ramo das FFAA possui no domínio da cibersegurança.

Com base nas entrevistas realizadas e nos documentos em referência do EMA e do EMGFA, nas várias vertentes da metodologia NATO, destaca-se o Pessoal, como um dos fatores mais importantes no desenvolvimento da ciberdefesa e como o mais crítico que a Marinha possui e necessita de promover. Os domínios da Doutrina, da Organização, do Treino, do Material e da Liderança também foram indicados como relevantes. Embora com o destaque de certos domínios, realça-se que a respetiva abordagem é caracterizada pela indissociabilidade dos seus elementos.

No Pessoal existem várias lacunas que tornam este domínio tão crítico para a Marinha. São elas a escassez de recursos humanos, a baixa capacidade de atrair e reter elementos, os ciclos curtos de gestão do pessoal nos cargos de Marinha, a falta de formação adequada e a pouca consciencialização dos utilizadores e das chefias para os perigos do ciberespaço e para a criação de hábitos que permitam prevenir as ameaças criadas por e neste meio.

Ao nível da Doutrina, é de notar que a Marinha apresenta publicações doutrinárias bastante desatualizadas e sem estarem harmonizadas com a atual organização para a ciberdefesa, nem com a doutrina NATO e da UE. Segundo o Comandante Neves, estas não compõem "formalmente nenhuma Doutrina", sendo na realidade "documentos enquadradores da organização" dos vários temas a que se sujeitam.

Ainda assim, para a Doutrina, na vertente da cibersegurança, destacam-se os seguintes documentos doutrinários nacionais, a Estratégia Nacional de Segurança do Ciberespaço 1.0, da qual foi publicada recentemente a sua nova versão 2.0, e a Lei n.º 46/2018, de 13 de agosto.

Na Estratégia 1.0, levantou-se a questão se a generalidade e a grande amplitude das medidas com que se poderiam atingir os seus objetivos, não poderiam criar ambiguidade e suscetibilidade ao erro e à dúvida. Foi também questionado o facto de nem todos os eixos serem aplicados às FFAA, embora se adequassem a esta organização, recebendo apenas uma visão de órgão responsável pela ciberdefesa.

De facto, constatou-se que a Estratégia 1.0 "não teve um plano de ação claro" (Jesus, 2019) e, enquanto estratégia, encontra-se a um nível macro, criando a necessidade de elaborar um plano de ação com a definição concreta de ações a cumprir por cada entidade (Marques, 2019; Jesus, 2019).

A intervenção da Estratégia 1.0 nas FFAA unicamente nas linhas orientadoras que dizem respeito ao desenvolvimento da capacidade de ciberdefesa, ou seja, excluindo o fator da cibersegurança da organização e a sua influência na segurança do ciberespaço nacional, foi também apontado como um fator impeditivo do desenvolvimento da capacidade de ciberdefesa da Marinha.

No entanto, estes aspetos foram revistos e assegurados na formulação da segunda versão da Estratégia, "efetuada de um modo muito mais participativo do que tinha sido a primeira" e "atualizada no que concerne a outras componentes do seu princípio fundamental" (Marques, 2019). A avaliação anual da mesma e sua revisão, visa a melhoria das suas vulnerabilidades e a sua adaptação ao paradigma digital em constante evolução, contemplando as vertentes necessárias à capacitação do país para garantir a

segurança do ciberespaço e pelas quais a Marinha é responsável por cumprir com determinadas medidas e atividades.

Especificamente para a Marinha, a ENSC 2.0 será uma mais valia por promover a segurança do seu ciberespaço de interesse, e por isso, na sua capacidade de ciberdefesa, terá um maior desenvolvimento se forem assegurados os domínios da metodologia NATO apresentados, com especial destaque para os que se apresentam mais críticos.

A Lei n.º 46/2018, de 13 de agosto, estabelece que não se aplica às redes e sistemas de informação diretamente relacionados com o C2 do EMGFA e dos ramos das FFAA, nem às redes e sistemas de informação que processem informação classificada, no entanto aplica-se a todo o restante universo de redes e sistemas das mesmas. De acordo com a lei, a Marinha deve cumprir com medidas pré-definidas que reforcem a seguranças das suas redes e sistemas e, em caso de ocorrência de incidentes relevantes, notificar o CNCS.

Pelas incumbências que a DIRCSI tem, enquanto autoridade técnica para a ciberdefesa e para a cibersegurança setorial, questionou-se a possível sobreposição das suas competências aos poderes de autoridade da ANC, sobre as redes e sistemas de informação da Defesa, no domínio de ambos os documentos legislativos. Segundo os entrevistados não parece haver sobreposição às mesmas (Marques, 2019; Jesus, 2019; Assunção, 2019), contudo, é uma questão que deverá ser analisada de acordo com cada caso, acautelando que a mesma lei "não prejudica as medidas destinadas a salvaguardar as funções essenciais do Estado" (Lei n.º 46/2018, de 13 de agosto).

A Lei n.º 46/2018, de 13 de agosto, constitui-se como mais um instrumento e um passo na promoção da segurança do ciberespaço nacional, estabelecendo o regime jurídico do mesmo. No entanto, para a Marinha, não será propriamente a lei que constituirá um fator de grande impacto na capacidade de assegurar a segurança do seu ciberespaço de interesse. Para tal, concorrem as medidas de ação propostas pelo MDN/EMGFA/CCD e o conjunto das vertentes que constituem uma capacidade que permitem cumprir com as mesmas, ressalvando para a "liderança, organização e meios humanos e materiais adequados" (Marques, 2019).

Ainda assim, os requisitos de segurança que a lei obriga a identificar na Marinha, competem para o conhecimento situacional das suas vulnerabilidades e das medidas a assegurar para as reforçar. Pelo atraso ocorrido na definição e publicação dos requisitos de segurança e de notificação de incidentes mencionados nesta lei, não foi possível realizar uma correta análise à sua aplicabilidade e impacto na Marinha, podendo-se retirar apenas conclusões gerais.

No decorrente do levantamento da capacidade operacional que a Marinha possui no domínio da cibersegurança, revelam-se algumas vulnerabilidades. Como referido a doutrina encontra-se desatualizada e além disso, é inexistente no âmbito de procedimentos e ações específicas a concretizar na ciberdefesa; na organização, certos cargos com funções na segurança das redes e sistemas são em acumulação; o treino e a formação do pessoal não se mostra ainda completo e adequado a todos os intervenientes; a comunidade utilizadora e os líderes deveriam estar mais sensibilizados e conscientes para os perigos e medidas de prevenção; existe uma enorme carência em recursos humanos; e algum material encontra-se em estado obsoleto.

Contudo, é possível destacar determinadas linhas de ação que promovem o desenvolvimento da capacidade de ciberdefesa. Sendo elas, o presente esforço de atualização das publicações doutrinárias de Marinha; as medidas e atividades derivadas da Estratégia e a sua atualização onde já são consideradas e corrigidas, numa análise primitiva, as questões colocadas neste trabalho; a crescente participação da Marinha em diversos eixos de treino e formação para o seu pessoal; as intenções de aumentar ações de sensibilização ao utilizadores das redes e sistemas de Marinha e as várias medidas adotadas e atividades onde o ramo participa, nacional e internacionalmente, e que contribuem para a interoperabilidade.

É notória a preocupação que a Marinha tem revelado no domínio da ciberdefesa, especialmente desde o ano de 2018, confluindo-se nos pontos expostos ao longo deste trabalho. Para tal, a NATO e a UE tiveram e têm uma grande influência. Estas organizações colaboraram através de diretivas, incentivos orçamentais, ações de treino e outras medidas.

Importa novamente realçar que as características que acompanham o ciberespaço são um fator importante neste domínio. Ao ser um espaço que apresenta uma constante e crescente evolução acompanhada de um maior número de ameaças com consequências cada vez mais devastadoras, os requisitos de segurança das redes e sistemas devem estar em conformidade com estes, por forma a assegurar uma eficaz e eficiente garantia da segurança do ciberespaço.

Neste sentido, é possível afirmar que atualmente a Marinha possui os requisitos necessários que lhe permitem responder às situações de incidentes de segurança no ciberespaço (Jesus, 2019; Neves, 2019; Carvalho, 2019; Prates, 2019). Embora com poucos recursos e não sendo os desejados, são os suficientes para cumprir com as suas competências numa primeira intervenção (Jesus, 2019). Numa situação mais crítica, ter-

se-á de "recorrer a uma resposta integrada das Forças Armadas", à semelhança dos outros ramos.

Embora não seja o foco deste trabalho, é relevante referir, que enquanto ramo das FFAA, a sua capacidade de ciberdefesa deverá incluir a área ofensiva e de exploração do ciberespaço. Pelos entrevistados, conclui-se que atualmente, a Marinha não possui capacidades a este nível, no entanto, é um objetivo futuro a cumprir e que se encontra vertido no *Plano de ação para o reforço da ciberdefesa da marinha* e na ENSC 2.0. Este tema, constituía igualmente, um objetivo a ser concretizado através de várias medidas definidas na ENSC 1.0 e que não se verificaram.

Por último, importa referir que o *Plano de ação para o reforço da ciberdefesa da Marinha*, constitui um fator de progresso no desenvolvimento da capacidade de ciberdefesa deste ramo, em conformidade com o exposto no *Plano de desenvolvimento da capacidade de ciberdefesa*, que de uma forma geral, a promove para as FFAA. O plano de ação desenvolvido pelo EMA, identifica as vulnerabilidades que a Marinha detém na sua capacidade e propõem medidas que permitam colmatar as mesmas, por forma a assegurar uma maior resiliência no ciberespaço (Carvalho, 2019; Prates, 2019).

Em título conclusivo, a Marinha apresenta ainda diversas lacunas, onde se destacam os recursos humanos e a comunidade utilizadora, podendo afirmar-se que são as pessoas e a sua capacitação o mais relevante na atualidade para aplicação neste meio. As linhas de ação da Estratégia permitiram o desenvolvimento de medidas de segurança do ciberespaço e a ENSC 2.0 veio complementar e atualizar a anterior, beneficiando a Marinha a este nível. As medidas e atividades realizadas na Marinha possibilitaram um reforço da sua capacidade. Contudo, esta não se verifica totalmente adaptada à evolução do ciberespaço e para os ataques proferidos neste e por este meio. Ainda assim, pode-se concluir que a Marinha Portuguesa possui uma capacidade de cibersegurança edificada e já algo desenvolvida, que se revela inerentemente, na sua capacidade de ciberdefesa, com alguns pontos ainda por melhorar e com o compromisso de uma postura mais ativa na sua adaptação ao ciberespaço e à doutrina NATO.

Sugestões para Trabalho Futuros

Embora com os atuais investimentos na capacidade de cibersegurança da Marinha, estes poderão não ser suficientes para reduzir os riscos existentes a este nível. Neste sentido, é relevante ter um conhecimento situacional adequado e atualizado para fornecer

à Marinha a total perceção das suas vulnerabilidades e aspetos a melhorar. Deste modo, sugere-se a realização contínua de estudos, nos moldes do presente trabalho, sobre a capacidade de cibersegurança da Marinha, permitindo também ter a noção da sua evolução.

Neste seguimento, poder-se-á complementar o presente trabalho com a capacidade que a Marinha possui na ciberdefesa, conciliando com os restantes ramos das FFAA e a direção e coordenação do CCD. Isto tendo em conta que a Marinha ainda não tem capacidade de exploração e ofensiva no ciberespaço, cabendo ao CCD esta competência em articulação com a NATO.

Para trabalhos futuros sugere-se ainda a análise da Lei n.º 46/2018, de 13 de agosto, na sua aplicabilidade e competências nas FFAA e especificamente na Marinha. Com o seu estudo, poder-se-á responder mais assertivamente às questões levantadas no desenvolvimento deste trabalho e, possivelmente, levantar outras.

Para terminar, sugere-se a análise das medidas e atividades que as FFAA deverão concretizar pelo estabelecido no futuro Plano de Ação que coaduna a ENSC 2.0. Dentro de cada eixo, seria importante conhecer que resultados trariam às mesmas. Seria proveitoso e útil para a identificação de possíveis questões na sua aplicabilidade na Marinha.

Bibliografia e Referências Bibliográficas

Academia Militar. (2017). Multinational Cyber Defense Education and Training Project (MN CD E&T) NATO Smart Defence Project 1.36. Retrieved January 28, 2019, from https://academiamilitar.pt/2-uncategorised/466-multinational-cyber-defense-education-and-training-project-mn-cd-e-t.html

Agence Nationale de la Sécurité des Systèmes d'Information. (2011). *Information systems defence and security France's strategy*. Retrieved from https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

Assembleia Constituinte. (1976). *Constituição da República Portuguesa - V Revisão Contitucional*.

Assembleia da República. Lei n.º 109/2009 de 15 de setembro. Lei do Cibercrime (2009). Diário da República, 1.ª série — N.º 179 — 15 de Setembro de 2009. Retrieved from https://dre.pt/pesquisa/-/search/489693/details/maximized

Assembleia da República. Lei Orgânica n.º 6/2014 de 1 de setembroL. ei Orgânica de Bases da Organização das Forças Armadas (2014). Diário da República n.º 167/2014, Série I de 2014-09-01. Retrieved from https://dre.pt/pesquisa/-/search/56384929/details/maximized?print_preview=print-preview

Assembleia da República. Lei n.º 46/2018 de 13 de agosto (2018). Diário da República n.º 155/2018, Série I de 2018-08-13. Retrieved from https://dre.pt/pesquisa/-/search/116029384/details/maximized

Assembleia da República. Lei n.º 58/2019 de 8 de agosto, Pub. L. No. Diário da República n.º 151/2019, Série I de 2019-08-08 (2019). Retrieved from https://dre.pt/web/guest/pesquisa/-/search/123815982/details/maximized

Avast. (n.d.-a). Petya. Retrieved June 14, 2019, from https://www.avast.com/pt-br/c-petya

Avast. (n.d.-b). WannaCry. Retrieved June 14, 2019, from https://www.avast.com/pt-br/c-wannacry

Capacidade de Resposta a Incidentes de Segurança da Informação. (n.d.). Retrieved May 25, 2019, from

https://intranet.marinha.pt/subportais/Colaborativos/CRISI/Paginas/CRISI.aspx#

Carvalho, R. de. (2017). Ciberespaço: O quinto domínio operacional. *Revista Da Armada, 518*, 16, 17. Retrieved from https://www.marinha.pt/Conteudos_Externos/Revista_Armada/2017/518/index.html#p=17

Castells, M. (1999). *A Era da Informação: economia, sociedade e cultura, vol 3*. São Paulo: Paz e terra.

Castells, M. (2003). *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahan.

Castells, M. (2007). *A Era da Informação: Economia, Sociedade e Cultura - vol. I. A Sociedade em Rede*. (F. C. Gulbenkian, Ed.).

CCDCOE. (n.d.-a). CCD COE. Retrieved January 20, 2019, from https://ccdcoe.org/nato.html

CCDCOE. (n.d.-b). Cyber Definitions. Retrieved November 9, 2018, from https://ccdcoe.org/cyber-definitions.html

CCDCOE. (n.d.-c). Exercises. Retrieved January 16, 2019, from https://ccdcoe.org/exercises/

CCDCOE. (n.d.-d). Publications. Retrieved May 31, 2019, from https://ccdcoe.org/library/publications/

CCDCOE. (2017). Locked Shields. Retrieved January 16, 2019, from https://ccdcoe.org/locked-shields-2017.html

CCDCOE. (2018). Portugal to Join the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. Retrieved May 5, 2019, from https://ccdcoe.org/news/2018/portugal-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-Tallinn/

CCDCOE. (2019). Locked Shields. Retrieved May 5, 2019, from https://ccdcoe.org/exercises/locked-shields/

CEMA. (2018). Despacho do Almirante Chefe do Estado-Maior da Armada, n.º 59/18, de 11 de dezembro. In *Ordem da Armada N.º 56 - 12 de dezembro de 2018*. Retrieved from https://intranet.marinha.pt/comnicacaointerna/ordens/OA1/Lists/ArquivoOA1/2018/OA1_056_18.pdf

Centro Criptológico Nacional. (2015). GUÍA DE SEGURIDAD (CCN-STIC-401) - Glosario y Abreviaturas. Retrieved December 27, 2018, from https://www.ccn-

cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=193.html

Chen, T. M., & Robert, J.-M. (2004). The evolution of viruses and worms. In *Statistical methods in computer security 1*. Statistical methods in computer security 1.

Clarke, R. A., & Knake, R. K. (2012). *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins.

CNCS. (n.d.). Transposição da Diretiva NIS/SRI. Retrieved January 26, 2019, from https://www.cncs.gov.pt/transposicao-da-diretiva-nissri/

CNCS. (2018a, January 30). Cyber SOPEx para a cooperação CSIRT. *CNCS*. Retrieved from https://www.cncs.gov.pt/recursos/noticias/cyber-sopex-para-a-cooperacao-csirt/

CNCS. (2018b, June 7). Termina hoje o Cyber Europe 2018. *CNCS*. Retrieved from https://www.cncs.gov.pt/recursos/noticias/termina-hoje-o-cyber-europe-2018/

CNCS. (2019, April 8). Exercício Nacional de Cibersegurança termina com balanço positivo. *CNCS*. Retrieved from https://www.cncs.gov.pt/recursos/noticias/exercicio-nacional-de-ciberseguranca-termina-com-balanco-positivo/

Comissão das Comunidades Europeias. COM(2001)298 final. Segurança das redes e da informação: Proposta de abordagem de uma política europeia (2001). Retrieved from http://ec.europa.eu/transparency/regdoc/rep/1/2001/PT/1-2001-298-PT-F1-1.Pdf

Comissão das Comunidades Europeias. COM(2006) 251 final. Estratégia para uma sociedade da informação segura – "Diálogo, parcerias e maior poder de intervenção" (2006). Retrieved from http://ec.europa.eu/transparency/regdoc/rep/1/2006/PT/1-2006-251-PT-F1-1.Pdf

Comissão e Alta Representante. JOIN(2017) 450 final. Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE (2017). Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

Comissão Europeia. (n.d.-a). Decisão (UE, Euratom) 2015/444, de 13 de março de 2015, relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE. Retrieved June 22, 2019, from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:JOL_2015_072_R_0011&qid=1427204240846&from=PT

Comissão Europeia. (n.d.-b). Objetivos gerais da União Europeia. Retrieved January 20,

2019, from https://ec.europa.eu/info/strategy/priorities-and-goals/overall-goals-eu_pt

Comissão Europeia. (n.d.-c). Reforma de 2018 das regras de proteção de dados da UE. Retrieved May 5, 2019, from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_pt#sobreoregulamentoeaproteodedados

Comissão Europeia. JOIN(2013) 1 final. Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido, Pub. L. No. JOIN(2013) 1 final (2013). Bruxelas.

Comissão Europeia. COM(2016) 410 final. Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora (2016). Retrieved from https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:52016DC0410

Comissão Europeia. (2016b). *Comissão assina um acordo com a indústria sobre cibersegurança e intensifica os esforços para combater as ciberameaças*. Bruxelas. Retrieved from http://europa.eu/rapid/press-release_IP-16-2321_pt.htm

Comissão Europeia. COM(2017) 477 final. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulame (2017). Bruxelas. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-477-F1-PT-MAIN-PART-1.PDF

Comissão Europeia. COM(2017) 489 final. Proposta de Diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho (2017). Bruxelas. Retrieved from https://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-489-F1-PT-MAIN-PART-1.PDF

Comissão Europeia. Recomendação (UE) 2017/1584 da Comissão de 13 de setembro de 2017 sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (2017). Jornal Oficial da União Europeia. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017H1584&from=EN

Comissão Europeia. SWD(2018) 404 final. Resumo da Avaliação de Impacto que acompanha o documento Proposta de Regulamento que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a

Rede de Centros Nacionai (2018). Bruxelas. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52018SC0404

Conselho da UE. Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018) (2018). Bruxelas. Retrieved from http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/pt/pdf

Conselho da União Europeia. Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013 relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (2013). Jornal Oficial da União Europeia. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:PT:PDF

Conselho da União Europeia. DECISÃO (PESC) 2015/1835 do Conselho de 12 de outubro de 2015 que define o estatuto, a sede e as regras de funcionamento da Agência Europeia de Defesa (reformulação) (2015). Jornal Oficial da União Europeia. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015D1835&from=en

Conselho da União Europeia. Decisão (PESC) 2018/712 do Conselho, de 14 de maio de 2018, que altera a Decisão (PESC) 2016/2382 que cria a Academia Europeia de Segurança e Defesa (AESD) (2018). Jornal Oficial da União Europeia. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1548619295277&uri=CELEX:32018D0712

Conselho de Ministros. (2019, May 23). Comunicado do Conselho de Ministros de 23 de maio de 2019. *República Portuguesa*. Retrieved from https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278

Conselho Europeu, & Conselho da UE. (2019). Reforma da cibersegurança na Europa. Retrieved January 28, 2019, from https://www.consilium.europa.eu/pt/policies/cyber-security/

Council of Europe. Convention on Cybercrime (2001). Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Crawford, S. (1983). *The Origin and Development of a Concept: The Information Society*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC227258/pdf/mlab00068-0030.pdf

Cunha, G. A. da. (2018, January). Segurança Nacional e Defesa Nacional no Estado de Direito Democrático. *Revista Militar*. Retrieved from

http://www.revistamilitar.pt/artigopdf/1298

Defending against cyber attacks. (n.d.). Retrieved February 15, 2019, from http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf

Defesa Nacional - Gabinete do Ministro. Despacho n.º 9762/2017 de 9 de novembro (2017). Diário da República n.º 216/2017, Série II de 2017-11-09. Retrieved from https://dre.pt/web/guest/home/-/dre/114163969/details/1/maximized?serie=II&print_preview=print-preview&day=2017-10-26&date=2017-10-01&dreId=114163953

Diretiva Estratégica da Marinha 2018. (2018). Retrieved from https://www.marinha.pt/conteudos_externos/Diretiva_Estrategica_da_Marinha/PDF/DEM_2018.pdf

Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2018-2021. (2018). Retrieved from https://www.emgfa.pt/documents/435jnqg1vmd7.pdf

DITIC-NCIRC. (n.d.). Organograma. Retrieved March 6, 2019, from https://intranet.marinha.pt/subportais/STI/DITIC/Paginas/Organograma.aspx

DITIC-NCIRC. (2018). *Conceitos de Cibersegurança*. Lisboa.

Documentos. (n.d.). Retrieved May 31, 2019, from https://intranet.marinha.pt/subportais/Colaborativos/CRISI/doc/Paginas/default.aspx

Dossier de Curso - Curso de Aperfeiçoamento em Conceitos Gerais de Cibersegurança AKS70. (n.d.). Escola de Tecnologias Navais. Retrieved from https://intranet.marinha.pt/subportais/SP/DirecaoFormacao/atividadesdeformacao/Lists/Ficheiros/ETNA/AKS70 CURSO DE APERFEIÇOAMENTO EM CONCEITOS GERAIS DE CIBERSEGURANÇA LOMB 1040.pdf

EMA. (2005). *PCA 2 (B) - Doutrina para os Sistemas de Informação e Comunicação Automatizados (SICA) na Marinha*. Ministério da Defesa Nacional.

EMA. (2006). *PDA 2 - Glossário de Sistemas e Tecnologias de Informação e Comunicação (GlosSTIC)*. Ministério da Defesa Nacional.

EMA. (2012). *PCA 16 - Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha*. Ministério da Defesa Nacional.

EMGFA. (n.d.). CMX - Crisis Management Exercise. Retrieved June 1, 2019, from https://www.emgfa.pt/pt/operacoes/exerc/cmx2

EMGFA. (2017a, July 3). Forças Armadas Portuguesas participam no maior exercício de

interoperabilidade da NATO - CWIX. *Estado-Maior-General Das Forças Armadas*. Retrieved from https://www.emgfa.pt/pt/noticias/1092

EMGFA. (2017b, November 7). 1º Exercicio Ciberdefesa Ibero-Americano. *Estado-Maior-General Das Forças Armadas*. Retrieved from https://www.emgfa.pt/pt/noticias/1112

EMGFA. (2018a, April 23). Portugal junta-se ao grupo de países NATO mais avançados em ciberdefesa. *Estado-Maior-General Das Forças Armadas*. Retrieved from https://www.emgfa.pt/pt/noticias/1183

EMGFA. (2018b, November 27). Forças Armadas participam no maior exercício de ciberdefesa da NATO. *Estado-Maior-General Das Forças Armadas*. Retrieved from https://www.emgfa.pt/pt/noticias/1296?fbclid=IwAR09MNTKOFhwLspAizz8IsQ2XoJqkJeQQBFfiLX0KS2eC_mbFi_JpdqLOBE

EMGFA. (2019, April 11). Portugal participa no maior e mais complexo exercício de ciberdefesa internacional. *Estado-Maior-General Das Forças Armadas*. Retrieved from https://www.emgfa.pt/pt/noticias/1362

ENISA. (n.d.). CSIRTS in Europe. Retrieved January 23, 2019, from https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building/european-initiatives/cert-eu

ENISA. (2018a). Cyber Europe. Retrieved January 23, 2019, from https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

ENISA. (2018b). ENISA organises cyber-exercise to boost CSIRT cooperation. *ENISA*. Retrieved from https://www.enisa.europa.eu/news/enisa-news/enisa-organises-cyber-exercise-to-boost-csirt-cooperation

European Comission. (2019). Cybercrime. Retrieved January 22, 2019, from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

European Commission. (2017a). *European Commission - Speech PRESIDENT JEAN-CLAUDE JUNCKER'S State of the Union Address 2017*. Brussels. Retrieved from http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm

European Commission. (2017b). Special Eurobarometer 464a - Europeans' attitudes towards cyber security. Retrieved December 26, 2018, from ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/yearFrom/2016/yearTo/2017/search/cyber/surveyKy/2171%0D

European Defence Agency. (2015). Cyber Defence. Retrieved from

https://www.eda.europa.eu/docs/default-source/eda-factsheets/2014-03-24-factsheet_cyber_defence_high-

Europeia, C. da U. (2014). *Quadro Estratégico da UE em matéria de Ciberdefesa*. Bruxelas. Retrieved from http://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/pt/pdf

EUROPOL. (n.d.). Sobre a EUROPOL. Retrieved January 22, 2019, from https://www.europol.europa.eu/pt/about-europol

Exército Português. (n.d.). Multinational Cyber Defence Education and Training Project (MN CD E&T) NATO SMART DEFENCE PROJECT 1.36. Retrieved May 31, 2019, from https://mncdet.wixsite.com/mncdet-nato

Exército Português. (2018, November 14). EXERCÍCIO CIBER PERSEU. *Exército Português*. Retrieved from https://www.exercito.pt/pt/informação-pública/comunicados/172

Freire, F. V., & Nunes, P. V. (2013). *Estratégia da Informação e Segurança no Ciberespaço*. (A. Carriço, Ed.). Lisboa: Instituto da Defesa Nacional.

Gabinete Nacional de Segurança, & Centro Nacional de Cibersegurança. (2018). *Avaliação da Execução da Estratégia Nacional de Segurança do Ciberespaço – 2018*.

Geers, K. (2008). Cyberspace and the Changing Nature of Warfare. *SC Magazine*. Retrieved from https://ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf

Gelbstein, E. (2012). Appendix 1 Basic information security definitions and terminology. In A. Carriço (Ed.), *Cibersegurança*. Lisboa: N.º 133, IDN.

Geraldes, A. R. da S. V. (2013). *Ciberterrorismo - cenário de materialização*.

Gibson, W. (1984). *Neuromancer* (1st ed.). Ace.

GlossaryTech. (n.d.). GlossaryTech: General Terms. Retrieved January 11, 2019, from https://glossarytech.com/terms/general_terms

GNS. Glossário de termos técnicos de segurança, SEGNAC 2. Retrieved from https://www.gns.gov.pt/media/11027/glossario_seguranca.pdf

GT-CCFA. (2018). *Plano de Desenvolvimento da Capcidade de Ciberdefesa*.

GT-EMA. (2018). *Plano de Ação para o Reforço da Ciberdefesa da Marinha*.

Hughes, R. B. (2009). *NATO and Cyber Defence* (4 No. 1). Retrieved from https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

Instituto Universitário Militar. (n.d.). Curso de Planeamento de Operaçõe de Ciberdefesa (CPOCIBER). Retrieved May 26, 2019, from https://www.ium.pt/s/index.php/pt/cursos/cursos-de-especializacao/curso-de-planeamento-de-operacoes-de-ciberdefesa-cpociber

Jornal Oficial da União Europeia. (2018). Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva . *Jornal Oficial Da União Europeia*. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2018:127:FULL&from=PT#%FE%FF%00O%00J%00X%000%000%000%002%000%001%00P%00T

Lévy, P. (1999). *Cibercultura* (1st ed.). São Paulo: Editora 34. Retrieved from https://mundonativodigital.files.wordpress.com/2016/03/cibercultura-pierre-levy.pdf

Maurer, T., & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*. New America. Retrieved from https://www.giplatform.org/sites/default/files/Compilation of Existing Cybersecurity and Information Security Related Definition.pdf

Ministério da Defesa Nacional. Despacho 13692/2013 de 28 de outubro. Orientação Política para a Ciberdefesa (2013). Lisboa: Diário da República, 2.ª série— N.º 208, de 28 de outrubro de 2013

Ministério da Defesa Nacional. DL n.º 184/2014 de 29 de dezembro. Lei Orgânica do Estado-Maior General das Forças Armadas (2014). Diário da República n.º 250/2014, Série I de 2014-12-29. Retrieved from https://dre.pt/pesquisa/-/search/65983261/details/maximized

Ministério da Defesa Nacional. Decreto Regulamentar n.º 10/2015, de 31 de julho (2015). Diário da República n.º 148/2015, Série I de 2015-07-31. Retrieved from https://dre.pt/home/-/dre/69920322/details/maximized?p_auth=ClJVY0jO

Ministério da Defesa Nacional. Decreto Regulamentar n.º 13/2015 de 31 de julho (2015). Diário da República n.º 148/2015, Série I de 2015-07-31. Retrieved from https://dre.pt/home/-/dre/69920325/details/maximized?p_auth=ClJVY0jO

Ministérios do Trabalho e da Segurança Social, da Educação e da Ciência, T. e E. S. Portaria n.º 782/2009, de 23 de julho (2009). Retrieved from https://dre.pt/pesquisa/-/search/493227/details/normal?q=Portaria+n.º 782/2009https://dre.pt/pesquisa/-

/search/493227/details/normal?q=Portaria+n.º 782/2009

Moniz, P. (2018). Impacto do Ciberespaço na Sociedade em Rede. In *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: N.º 28, IDN.

Monteiro, S. (2016, May). Cibersegurança e ciberdefesa − Portugal e NATO. *Revista Da Armada*, pp. 4, 5. Retrieved from https://www.marinha.pt/Conteudos_Externos/RevistaArmada/_FlipVersion/2016/507/files/assets/basic-html/page5.html

NATO. (n.d.). O que é a NATO? Retrieved January 14, 2019, from https://www.nato.int/nato-welcome/index_pt.html

NATO. (1949). *Tratado do Atlântico Norte*. Washington D.C. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt

NATO. (2002). Prague Summit Declaration. Retrieved January 14, 2019, from https://www.nato.int/cps/en/natohq/official_texts_19552.htm?selectedLocale=en

NATO. (2006). Riga Summit Declaration. Retrieved January 17, 2019, from https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en

NATO. (2007). Final Communiqué. Retrieved January 18, 2019, from https://www.nato.int/cps/en/natohq/news_47011.htm?selectedLocale=en

NATO. (2008). Bucharest Summit Declaration. Retrieved January 19, 2019, from https://www.nato.int/cps/en/natohq/official_texts_8443.htm?selectedLocale=en

NATO. (2012). Chicago Summit Declaration. Retrieved January 17, 2019, from https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

NATO. (2014a). Cyber Security Strategy for Defence. Retrieved November 11, 2018, from https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=193.html

NATO. (2014b). Wales Summit Declaration. Retrieved January 17, 2019, from https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

NATO. (2016a). Cyber Defence Pledge. Retrieved January 19, 2019, from https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en

NATO. (2016b). Statement. Retrieved January 19, 2019, from https://www.nato.int/cps/en/natohq/official_texts_138829.htm?selectedLocale=en

NATO. (2016c). Warsaw Summit Communiqué. Retrieved January 19, 2019, from https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

NATO. (2017a). Common set of new proposals. Retrieved January 19, 2019, from https://www.nato.int/cps/en/natohq/official_texts_149522.htm?selectedLocale=en

NATO. (2017b). Partnership Interoperability Initiative. *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/topics_132726.htm?selectedLocale=en

NATO. (2018a). *AAP-06 NATO Glossary of Terms and Definitions* (2018th ed.). NATO STANDARDIZATION OFFICE (NSO).

NATO. (2018b). Brussels Summit Declaration. Retrieved January 19, 2019, from https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en

NATO. (2018c). Education and training. Retrieved May 23, 2019, from https://www.nato.int/cps/en/natohq/topics_49206.htm

NATO. (2018d). NATO Cyber Defence. *NATO*. Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf

NATO. (2018e, July 16). Cyber defence. *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

NATO. (2019). *AAP-47 Allied Joint Doctrine Development* (C Version). NATO STANDARDIZATION OFFICE (NSO).

NCIA. (n.d.-a). About the NCI Agency. Retrieved January 17, 2019, from https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx

NCIA. (n.d.-b). Cyber Coalition. Retrieved May 4, 2019, from https://www.ncia.nato.int/NewsRoom/Pages/20181211-CyberCoalition.aspx

NCIA. (n.d.-c). Cyber Security. Retrieved January 17, 2019, from https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx

NCIA. (2017). NCIAcademy groundbreaking ceremony. Retrieved February 10, 2019, from https://www.ncia.nato.int/NewsRoom/Pages/170523-NCI-Academy_groundbreaking_ceremony.aspx

Neves, P. J. B. das. (2015). *Capacidade de Resposta a incidentes de segurança da informação no ciberespaço: Uma abordagem DOTMLPI-I*. Mestrado em Segurança da Informação e Direito no Ciberespaço por Escola Naval, Instituto Superior Técnico, Faculdade de Direito - Universidade de Lisboa.

Neves, P. J. B. das, & Correia, F. J. R. (2016). *Resposta a Incidentes de Segurança da Informação: Uma abordagem DOTMLPI-I* (No. 01).

Nunes, P. V. (2018). Introdução. In *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: N.º 28, IDN.

Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities* (Global Commission on Internet Governance Paper Series No. 1). Retrieved from

https://dash.harvard.edu/bitstream/handle/1/12308565/Nye-GlobalCommission.pdf

Parlamento Europeu e Conselho da União Europeia. Regulamento (CE) n.° 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004 (2004). Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32004R0460

Parlamento Europeu e Conselho da União Europeia. Diretiva (UE) 2016/1148 de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (2016). Jornal Oficial da União Europeia. Retrieved from https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT

Parlamento Europeu e Conselho da União Europeia. Regulamento (UE) 2016/679 de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (2016). Jornal Oficial da União Europeia. Retrieved from https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf

Portugal. (1997). *Livro Verde para a Sociedade da Informação em Portugal*. Retrieved from http://purl.pt/239/2/

Presidência do Conselho de Ministros. Decreto-Lei n.º 3/2012 de 16 de janeiro (2012). Diário da República n.º 11/2012, Série I de 2012-01-16. Retrieved from https://dre.pt/pesquisa/-/search/544575/details/maximized

Presidência do Conselho de Ministros. RCM n.º 19/2013 de 5 de abril. Conceito Estratégico de Defesa Nacional (2013). Diário da República n.º 67/2013, Série I de 2013-04-05. Retrieved from https://dre.pt/pesquisa/-/search/259967/details/maximized

Presidência do Conselho de Ministros. RCM n.º 26/2013 de 11 de abril. Defesa 2020 (2013). Diário da República n.º 77/2013, Série I de 2013-04-19. Retrieved from https://dre.pt/web/guest/pesquisa/-/search/260395/details/maximized

Presidência do Conselho de Ministros. Decreto-Lei n.º 69/2014 de 9 de maio (2014). Diário da República n.º 89/2014, Série I de 2014-05-09. Retrieved from https://dre.pt/pesquisa/-/search/25343754/details/maximized

Presidência do Conselho de Ministros. RCM n.º 36/2015 de 12 de junho. Estratégia Nacional de Segurança do Ciberespaço (2015). Diário da República n.º 113/2015, Série I de 2015-06-12. Retrieved from https://dre.pt/home/-/dre/67468089/details/maximized?p_auth=pKf7McIZ

Presidência do Conselho de Ministros. RCM n.º 115/2017, de 24 de agosto (2017). Diário da República n.º 163/2017, Série I de 2017-08-24. Retrieved from https://dre.pt/home/-/dre/108051990/details/maximized

Presidência do Conselho de Ministros. RCM n.º 92/2019 de 5 de junho. Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (2019). Diário da República n.º 108/2019, Série I de 2019-06-05. Retrieved from https://dre.pt/web/guest/home/-/dre/122498962/details/maximized

Presidência e da Modernização Administrativa. Decreto-Lei n.º 136/2017 de 6 de novembro (2017). Diário da República n.º 213/2017, Série I de 2017-11-06. Retrieved from https://dre.pt/home/-/dre/114152775/details/maximized

PS. (2019). *Projeto de Lei n.º 1217/XIII aprova a Carta de Direitos Fundamentais na Era Digital*. Retrieved from http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c3246795958427 74f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634770734d5449784e79315953556c4a4c6d527659773d3d&fich=pjl1217-XIII.doc&Inline=true

Quivy, R., & Campenhoudt, L. Van. (2005). *Manual de Investigação em Ciências Sociais*. (G. Valente, Ed.) (4th ed.). gradiva.

Ramos, H. (2013). *Ciberguerra: Apropriação da Tecnologia Hoje, Hegemonia das Nações Amanhã* (Observatorio). Retrieved from https://s3.amazonaws.com/academia.edu.documents/30612946/Ciberguerra__Apropriacao_da_Tecnologia_Hoje__Hegemonia_das_Nacoes_Amanha.pdf?response-content-disposition=inline%3B filename%3DCiberguerra_Apropriacao_da_Tecnologia_Ho.pdf&X-Amz-Algorithm=AWS4-HMAC-

Ramos, J. (2011). Primeiro vírus informático criado há 40 anos. *Expresso*. Retrieved from https://expresso.pt/economia/primeiro-virus-informatico-criado-ha-40-anos=f638343#gs.V9WnQq0, acedido a 02-01-2019

Regulamento Interno da Direção de Tecnologias de Informação e Comunicações. (2016). In *Despacho do Almirante Chefe do Estado-Maior da Armada n.º 50/2016, de 10 de maio*.

Regulamento Interno do Comando Naval. (2016). In *Despacho do Almirante Chefe do Estado-Maior da Armada n.º 61/2016, de 25 de maio*. Retrieved from https://www.marinha.pt/Conteudos_Externos/OrdensBD/OA1/Ficheiros/2016/23/R

I_CN.pdf

Resolução do Conselho de Ministros. RCM n.º 37/89 de 24 de outubro. Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Industrial Tecnológica e de Investigação - SEGNAC 2 (1989). Lisboa: Diário da República n.º 245/1989, Série I de 1989-10-24. Retrieved from https://dre.pt/pesquisa/-/search/549396/details/maximized?perPage=50&sort=whenSearchable&q=Lei+n.º 10%2F97&sortOrder=ASC%2Fen%2Fen%2Fen

Resolução do Conselho de Ministros. RCM n.º 5/90 de 28 de fevereiro. Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Informática - SEGNAC 4, Pub. L. No. Diário da República n.º 49/1990, 1º Suplemento, Série I de 1990-02-28 (1990). Retrieved from https://dre.pt/pesquisa-avancada/-/asearch/307435/details/maximized?perPage=100&anoDR=1990&types=SERIEI&search=Pesquisar

Resolução do Conselho de Ministros. RCM n.º 107/2003 de 12 de agosto. Plano de Acção para a Sociedade de Informação (2003). Lisboa: Diário da República — I Série-B N.º 185 — 12 /08/2003. Retrieved from https://dre.pt/application/dir/pdf1sdip/2003/08/185B00/47944832.pdf

Resolução do Conselho de Ministros. RCM n.º 12/2012 de 7 de fevereiro. Plano de Ação, Pub. L. No. Diário da República n.º 27/2012, Série I de 2012-02-07 (2012). Retrieved from https://dre.pt/pesquisa/-/search/543701/details/maximized

Rouse, M. (2019). Definition distributed denial of service (DDoS) attack. Retrieved February 5, 2019, from https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

Santos, D. G. G. (2014). *A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança*. ISCTE-IUL.

Santos, J. L. A. dos. (2011). *Contributos para uma melhor governação da cibersegurança em Portugal*. Universidade Nova de Lisboa: Faculdade de Direito. Retrieved from https://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF

Santos, J., Caetano, A., & Jesuíno, J. C. (2008). *As competências funcionais dos líderes e a eficácia das equipas* (Revista Portuguesa e Brasileira de Gestão). Retrieved from http://www.scielo.mec.pt/pdf/rpbg/v7n3/v7n3a04.pdf

Santos, L. (2012). Contribuições para uma melhor governação da Cibersegurança, vol 2.

In G. J. B. (Ed.), *Estudos de Direito e Segurança* (p. 2018). Lisboa: Edições Almedina.

Schmitt, M., Boothby, W., Demeyere, B., Heinegg, W., Michael, J., Wingfield, T., … Watts, S. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. (M. Schmitt, Ed.) (1st ed.). Cambridge University Press.

Schmitt, M., Boothby, W., Demeyere, B., Heinegg, W., Michael, J., Wingfield, T., … Watts, S. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. (M. Schmitt, Ed.) (2nd ed.). Cambridge University Press. Retrieved from https://www.parlamento.pt/Legislacao/paginas/constituicaorepublicaportuguesa.aspx

Shea, J. (2011). Cyber defence: next steps. Retrieved January 17, 2019, from https://www.nato.int/cps/en/natolive/news_75358.htm?selectedLocale=en

Singer, P., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know* (1st ed.). Oxford University Press.

Software de Suporte. (n.d.). Retrieved April 22, 2019, from https://intranet.marinha.pt/subportais/Colaborativos/CRISI/Suporte/Paginas/default.aspx

Techopedia. (n.d.). Techopedia: Firmware. Retrieved January 11, 2019, from https://www.techopedia.com/definition/2137/firmware

Theiler, O. (2011). Novas ameaças: a dimensão cibernética. *Revista Da NATO*. Retrieved from https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm

UK ESRC IAA Project Co-Creation. (2019). International Cyber Law in Practice: Interactive Toolkit. Retrieved June 18, 2019, from https://cyberlaw.ccdcoe.org/wiki/Main_Page

União Europeia, & United States. (2010). *EU-U.S. Summit 20 November 2010, Lisbon - Joint Statement*. Brussels. Retrieved from http://europa.eu/rapid/press-release_MEMO-10-597_en.htm

VdA Academia. (2018, April 12). VdA Academia integra consórcio para iniciativa da Cyber Academia and Innovation Hub. *VdA Academia*. Retrieved from http://www.vdacademia.pt/pt/iniciativas/noticias/VdA-Academia-integra-consorcio-para-iniciativa-da-Cyber-Academia-and-Innovation-Hub/280/

Veiga, P. (2018, July 2). O prefixo ciber. *Público*. Retrieved from

https://www.publico.pt/2018/07/02/tecnologia/opiniao/o-prefixo-ciber-1836304?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PublicoTecnologia+%28Publico.pt+-+Tecnologia%29

Viana, V. (2012). Editorial. In A. Carriço (Ed.), *Cibersegurança*. Lisboa: N.º 133, Instituto da Defesa Nacional.

Viana, V. (2018). Prólogo. In *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: N.º 28, IDN.

Apêndices

Os seguintes apêndices revelam as entrevistas realizadas a entidades com funções no campo da cibersegurança ou da ciberdefesa nacional. Os próximos textos transcrevem as questões e respostas realizadas por escrito. Pretendeu-se que as respostas fossem abertas e exprimissem a opinião do entrevistado sobre o tema em questão, tendo por base a sua experiência e o cargo desempenhado ou a desempenhar.

As questões foram realizadas com foco nas funções e competências dos respetivos, diferindo por esse motivo, no teor das entrevistas. Contudo, por forma a contextualizar o âmbito da dissertação, foi apresentado no guião de todas as entrevistas o seguinte parágrafo:

"Muitos dos serviços de ciberdefesa baseiam-se funcionalmente nas capacidades técnicas, tradicionalmente associadas à cibersegurança, que passam pela prevenção, deteção e recuperação dos SIC face à ocorrência de ataques cibernéticos". (Despacho 13692/2013 de 28 de outubro). É com base nesta abordagem que estou a desenvolver a minha dissertação e se referem as seguintes questões da entrevista. Ou seja, excluindo a área ofensiva e de exploração do ciberespaço.

Apêndice A – Entrevista ao Almirante Gameiro Marques (GNS/ANS)

O Contra-almirante Gameiro Marques desempenha atualmente as funções de Diretor Geral do Gabinete Nacional de Segurança e por inerência, de Autoridade Nacional de Segurança.

1. Para a edificação de uma capacidade operacional de ciberdefesa na Marinha Portuguesa pode ser considerada a metodologia DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade).

Doutrina – Relaciona-se com "os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum" (Neves & Correia, 2016).

Organização – Permite a constituição dos "indivíduos em equipas, e estas em unidades operacionais, para a execução coordenada das funções (…) [de modo a] atingirem os objetivos operacionais da organização" (Neves, 2015).

Treino – Visa preparar os "diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais (…) sendo relevante as lições aprendidas através do treino" (Neves, 2015).

Material – Composto por "tudo o que é necessário para suportar e equipar as unidades operacionais (…) ou seja, todo o material que tenha relevância para o sucesso da missão" (Neves & Correia, 2016).

Liderança – Refere-se "à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar (…) [dirigindo e motivando] os membros da equipa, (…) sabendo aproveitar eficazmente as mais-valias dos vários elementos" (Neves & Correia, 2016).

Pessoal – Compete "à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas" e garantir que estes possuem as qualificações necessárias para o desempenho da missão (Neves & Correia, 2016).

Infraestruturas – "Disponibilização de instalações adequadas à preparação e condução das operações" (Neves & Correia, 2016).

Interoperabilidade – Referente "à necessidade de interagir com parceiros externos, (…) que colaboram para atingir [o] mesmo objetivo" (Neves, 2015).

Com base nesta metodologia, quais/qual o(s) domínio(s) que considera mais relevante(s) e essenciais/essencial para o desenvolvimento da capacidade de ciberdefesa da Marinha e de que forma se destaca(m) dos restantes?

Resposta:

D, O, T, L e P.

2. A Estratégia Nacional de Segurança do Ciberespaço visa "aprofundar a segurança das redes e da informação (…) e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (RCM n.º 36/2015 de 12 de junho).

Os dados retirados da avaliação dos três anos evidenciam o comprometimento das várias entidades responsáveis em cumprir as linhas de ação definidas pela ENSC e mostram resultados positivos na sua concretização. No entanto, as "medidas e atividades da ENSC são (…) genéricas e de grande amplitude, podendo ser alcançadas de forma distintas" (GNS/CNCS, 2018).

Este fator tem de positivo a liberdade de ação para a adoção das medidas e atividades que melhor se adequem às organizações/empresas. Contudo, questiono-o se as mesmas não criam ambiguidade, tornando a sua avaliação demasiado abrangente para ser possível efetuar um controlo eficaz da operacionalização das medidas e atividades criadas. Dentro das medidas estabelecidas para cada eixo, não deveriam ser definidos também certos parâmetros a cumprir para não existir ambiguidades e ser menos suscetível à dúvida e ao erro?

Resposta:

Sem dúvida. Por essa razão, o Plano de Ação subjacente à ENSC 2.0 irá ter indicadores e metas para cada medida introduzida.

3. No estender da ENSC e pelas linhas de ação referidas pela mesma, a atuação das Forças Armadas é salientada enquanto organismo responsável pela ciberdefesa nacional e é nesse âmbito que vão de encontro as atividades propostas pelo EMGFA.

Contudo, existem outros eixos de intervenção e respetivas medidas concretas que se adequam igualmente às Forças Armadas enquanto organização, tal como o Eixo 4

– *Educação, sensibilização e prevenção*, mas que simultaneamente as respetivas atividades não se adequam bem às FFAA.

"Não será possível assegurar a ciberdefesa sem garantir também a segurança da informação que circula nos SIC" (Sistemas de Informação e Comunicações), "dependendo em grande medida do grau de sensibilização e consciencialização das organizações e das pessoas" (Despacho 13692/2013 de 28 de outubro).
Considera que a ENSC compreende as vertentes necessárias ao desenvolvimento da capacidade de ciberdefesa nas Forças Armadas?

Resposta:

Sim. O representante do MDN/EMGFA no Conselho Superior de Segurança do Ciberespaço, e o Chefe do Centro de Ciberdefesa contribuíram com medidas que se inserem em todos os eixos da ENSC 2.0.

4. A Estratégia prevê uma avaliação anual do cumprimento dos seus objetivos estratégicos e das linhas de ação, bem como a sua adaptação aos desafios impostos pela evolução digital.

Considerando a evolução das ciberameaças e o aumento exponencial dos ataques, considera que a ENSC é capaz responder eficazmente perante o atual paradigma digital? Quais são os fatores que aponta como limitadores e os mais difíceis de alcançar?

Resposta:

A primeira versão já não. Por isso encetámos o desenvolvimento da 2ª versão que foi efetuada de um modo muito mais participativo do que tinha sido a primeira e é atualizada no que concerne a outras componentes do seu princípio fundamental, refletido na visão: Que Portugal seja um país seguro e próspero através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade. Esse princípio é que a ENSC reflete um "*whole of society approach*".

5. Na sua generalidade, de que forma considera que a ENSC irá capacitar o país para garantir a segurança do seu ciberespaço? Considera que as medidas definidas na ENSC contemplam as vertentes necessárias para tal?

Resposta:

Sim, devidamente complementadas pelo que estiver vertido no Plano de ação. Nenhuma estratégia é relevante sem um plano de ação e a devida monitorização. Essa deverá ser feita por cada um e será realizada globalmente pelo CSSC.

6. Especificamente para a Marinha, como considera que a ENSC irá reforçar a sua capacidade de ciberdefesa?

Resposta:

Sim, desde que as necessárias componentes da capacidade que referi na resposta à pergunta 1 sejam acauteladas.

7. A Lei n.º 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço e irá definir em legislação complementar os requisitos de segurança para a Administração Pública (Art. 14.º e Art. 31.º), onde se insere as Forças Armadas.

A presente lei não se aplica às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas, nem às redes e sistemas de informação que processem informação classificada (Art. 2.º).

Já no Art.º 30 º do DL n.º 184, de 29 de dezembro de 2014, define-se a missão da DIRCSI - Direção de Comunicações e Sistemas de Informações, como apresentado de seguida:

"1 — A DIRCSI tem por missão planear, estudar, dirigir, coordenar e executar as atividades inerentes aos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) necessários ao exercício do comando e controlo nas Forças Armadas.

2 — A DIRCSI, no âmbito da ciberdefesa, tem por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas.

3 — A DIRCSI tem ainda por missão, no âmbito da cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação do restante universo da defesa nacional".

No âmbito das redes e dos sistemas de informação alvos da Lei n.º 46/2018 e das disposições apresentadas nas competências da DIRCSI, pode-se questionar a possível existência de uma sobreposição de competências aos poderes de autoridade da Autoridade Nacional de Cibersegurança sobre as redes e sistemas de informação das Forças Armadas?

Resposta:

Não me parece.

8. De que forma considera que esta Lei irá reforçar o cumprimento dos objetivos da Estratégia Nacional de Segurança do Ciberespaço?

Resposta:

Por que dá poderes ao CNCS, enquanto ANSC, para cumprir o estabelecido na Diretiva SRI pois estabelece o regime jurídico do ciberespaço em Portugal.

9. Especificamente para a Marinha, como considera que a presente Lei irá influenciar a capacidade de assegurar a segurança do seu ciberespaço?

Resposta:

A Lei nem tanto. O que vai contribuir para assegurar a segurança do seu ciberespaço (eu diria antes “do ciberespaço de interesse para o cumprimento da missão da Marinha”) é por um lado contribuir com medidas para o plano de ação global, a inscrever pelo MDN/EMGFA/CCD, e por outro ter a necessária liderança, organização e meios humanos e materiais adequados para as concretizar.

10. Sobre a necessária ligação entre a ciberdefesa e a cibersegurança como atividades de proteção de redes e sistemas de informação em âmbitos e objetivos confluentes, poderá considerar-se a cibersegurança nacional como base da ciberdefesa? Nesse caso, quais as formas de articulação entre cibersegurança e ciberdefesa?

Resposta:

Sim, a ciberdefesa, no conceito vertido na ENSC 2.0 (Ciberdefesa consiste na atividade que visa assegurar a defesa nacional no ou através do ciberespaço.) não se conseguirá executar sem a devida base de Cibersegurança (Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.)

A articulação faz-se a três níveis: estratégico no CSSC. Operacional ao nível do grupo G4 que inclui o CNCS, o CCD, a UNC3T da PJ e a unidade de Cibersegurança dos SIS. Tático pela ligação entre o CERT.PT (Departamento de Operações do CNCS) e o CSIRT da Defesa, por via direta ou pela rede nacional de CSIRTS.

Apêndice B – Entrevista ao Comandante Fialho de Jesus (CCD)

O Comandante Fialho de Jesus desempenha atualmente as funções de Diretor do Centro de Ciberdefesa do Estado-Maior General das Força Armadas. É ainda representante do Ministério da Defesa Nacional/ Estado-Maior General das Força Armadas no Conselho Superior de Segurança do Ciberespaço.

1. A Estratégia Nacional de Segurança do Ciberespaço visa "aprofundar a segurança das redes e da informação (…) e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (RCM n.º 36/2015 de 12 de junho).

Os dados retirados da avaliação dos três anos evidenciam o comprometimento das várias entidades responsáveis em cumprir as linhas de ação definidas pela Estratégia Nacional de Segurança do Ciberespaço e mostram resultados positivos na sua concretização. No entanto, as "medidas e atividades da ENSC são (…) genéricas e de grande amplitude, podendo ser alcançadas de forma distintas" (GNS/CNCS, 2018). Para o caso das FFAA, este fator tem de positivo a liberdade de ação para a adoção das medidas e atividades que melhor se adequam à organização.

Contudo, questiono-o se as mesmas não criam ambiguidade, tornando a sua avaliação demasiado abrangente para ser possível efetuar um controlo eficaz da operacionalização das medidas e atividades criadas. Dentro das medidas estabelecidas para cada eixo, não deveriam ser definidos também certos parâmetros a cumprir para não existir ambiguidades e ser menos suscetível à dúvida e ao erro?

Resposta:

A tua questão é pertinente, vista desse lado.

Esta ENSC 1.0, foi a primeira e não teve um plano de ação claro, onde os critérios que falas estivessem presentes. Assim, cada entidade responsável por cumprir as suas linhas de ação estabeleceu os seus próprios critérios.

A Nova ENSC, versão 2.0, assim que aprovada terá depois um Plano de ação, o qual deverá ser apresentado até 4 meses após a sua aprovação da ENSC 2.0. E aí já haverá um maior direcionamento das atividades, com responsáveis, datas, entregáveis…

Outro aspeto que importa perceber é o nível a que se está nesta abordagem das estratégias: Muito macro, ao nível de topo, sendo abrangente. Depois, a parte do plano de execução, já entra num nível abaixo, com a tal caracterização que é necessária, para evitar ambiguidades e ser mais fácil o seu controlo.

2. No estender da ENSC e pelas linhas de ação referidas pela mesma, a atuação das Forças Armadas é salientada enquanto organismo responsável pela ciberdefesa nacional e é nesse âmbito que vão de encontro as atividades propostas pelo EMGFA.

Contudo, existem outros eixos de intervenção e respetivas medidas concretas que se adequam igualmente às Forças Armadas enquanto organização, tal como o Eixo 4 – *Educação, sensibilização e prevenção*, mas que simultaneamente as respetivas atividades não se adequam bem às FFAA.

"Não será possível assegurar a ciberdefesa sem garantir também a segurança da informação que circula nos SIC" (Sistemas de Informação e Comunicações), "dependendo em grande medida do grau de sensibilização e consciencialização das organizações e das pessoas" (Despacho 13692/2013 de 28 de outubro).

Considera que a ENSC compreende as vertentes necessárias à edificação da capacidade de ciberdefesa/cibersegurança nas FFAA?

Resposta:

Efetivamente não estão consideradas todas as vertentes. Por essa mesma razão, na elaboração da ENSC 2.0 que decorreu o ano transato e que está para promulgação, a área da Defesa, está nos 6 eixos lá considerados.

3. Para a edificação da capacidade operacional de ciberdefesa na Marinha Portuguesa pode ser considerada a metodologia DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade).

Doutrina – Relaciona-se com "os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum" (Neves & Correia, 2016).

Organização – Permite a constituição dos "indivíduos em equipas, e estas em unidades operacionais, para a execução coordenada das funções (…) [de modo a] atingirem os objetivos operacionais da organização" (Neves, 2015).

Treino – Visa preparar os "diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais (…) sendo relevante as lições aprendidas através do treino" (Neves, 2015).

Material – Composto por "tudo o que é necessário para suportar e equipar as unidades operacionais (…) ou seja, todo o material que tenha relevância para o sucesso da missão" (Neves & Correia, 2016).

Liderança – Refere-se "à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar (…) [dirigindo e motivando] os membros da equipa, (…) sabendo aproveitar eficazmente as mais-valias dos vários elementos" (Neves & Correia, 2016).

Pessoal – Compete "à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas" e garantir que estes possuem as qualificações necessárias para o desempenho da missão (Neves & Correia, 2016).

Infraestruturas – "Disponibilização de instalações adequadas à preparação e condução das operações" (Neves & Correia, 2016).

Interoperabilidade – Referente "à necessidade de interagir com parceiros externos, (…) que colaboram para atingir [o] mesmo objetivo" (Neves, 2015).

Com base nesta metodologia, quais/qual o(s) domínio(s) que considera mais relevante(s) e essenciais/essencial para a capacidade de ciberdefesa das Forças Armadas e de que forma se destaca(m) dos restantes?

Resposta:

Os 8 vetores de Capacidade correspondem a uma abordagem por excelência na edificação de uma capacidade global. Todos eles são relevantes, daí a sua adoção. Mas é claro que os Recursos Humanos são o fator crítico de sucesso em qualquer organização, com especial incidência nesta área. São poucos os existentes e a sua formação é complexa, dispendiosa e leva muito tempo. O Vetor de capacidade Organização também é muito relevante, para a garantia da boa operação, de forma eficiente e eficaz, assim como o do treino, que deve ser individual e coletivo.

4. Com base na sua experiência, especialmente na sua participação no Grupo de Trabalho para a avaliação das atividades da ENSC, e tendo em conta o foco da minha dissertação ser a Marinha Portuguesa, questiono-o como considera que este ramo esteja preparado a nível da cibersegurança.

Julga que a Marinha possui as condições/requisitos necessários para garantir eficazmente a segurança do seu ciberespaço? Quais os fatores, no caso de existirem, que considera serem mais críticos neste âmbito?

Resposta:

A Marinha tem uma organização que lhe permite responder às situações de incidentes de segurança no Ciberespaço. Objetivamente não tem os recursos desejados, mas tem os possíveis, que lhe permitem uma primeira intervenção. Caso a situação escale, terá de se recorrer a uma resposta integrada das Forças Armadas, situação semelhante para os outros Ramos. Os fatores mais críticos são, como acima referidos, o nº de recursos humanos afetos a esta área e a sua capacitação. A doutrina está em fase de atualização, uma vez que a organização anteriormente estabelecida é diferente da atualmente em vigor, desde a criação do Centro de Ciberdefesa (CCD).

5. No Art. 30º do DL n.º 184/2014, de 29 de dezembro, é apresentado o seguinte:

"2 - A DIRCSI, no âmbito da ciberdefesa, tem por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas.

- A DIRCSI tem ainda por missão, no âmbito da cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação dos sistemas de informação do restante universo da defesa nacional."

Simultaneamente, a Lei n.º 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço, aplicando-se também às FFFAA.

Tendo em conta o seguinte:

"6 — A presente lei não se aplica:

a) Às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas;

b) Às redes e sistemas de informação que processem informação classificada."

Pode ser considerado uma sobreposição de competências aos poderes de autoridade da Autoridade Nacional de Cibersegurança sobre as redes e sistemas de

informação da Defesa que não as de comando e controlo ou as que processem informação classificadas?

Resposta:

A tua questão é pertinente. No entanto, ressalvo que o §8, refere:

"8 — A presente lei não prejudica as medidas destinadas a salvaguardar as funções essenciais do Estado, incluindo medidas de proteção da informação cuja divulgação seja contrária aos interesses de segurança nacional, à manutenção de ordem pública ou a permitir a investigação, a deteção e a repressão de infrações penais."

Por outro lado, uma situação que possa ocorrer, por exemplo, no IASFA, na parte da ADM, já a intervenção da ANC poderá fazer sentido, à luz da nova diretiva.

Assim, interpreto que esta questão, para o caso das FFAA, terá de ser analisada caso a caso.

6. Uma das competências da DIRCSI passa por definir os "sistemas de comando, controlo (...)"(a) do Nr. 5, Art. 30.º). A DIRCSI define também estes sistemas para a Marinha? Ou é o próprio ramo responsável por o fazer?

Resposta:

Outra questão bem colocada.

Relembro que o §1 do artº 30 estabelece que:

"A DIRCSI tem por missão planear, estudar, dirigir, coordenar e executar as atividades inerentes aos sistemas de informação (SI) e tecnologias de informação e comunicação (TIC) necessários ao exercício do comando e controlo nas Forças Armadas".

Leia-se conjunto, que é parte integrante da capacidade de 2 ou mais Ramos. E faz todo o sentido que haja uma coordenação para efeitos de interoperabilidade e economia de escala, entre outros fatores.

Agora, se os sistemas são específicos de cada Ramo, então aí serão estes a definir os seus requisitos operacionais.

Apêndice C – Entrevista ao Comandante Baptista das Neves (NCIRC)[53]

O Comandante Baptista das Neves desempenhou o cargo de Chefe do Núcleo *Computer Incident Response Capability* da Marinha, de 2016 até fevereiro de 2019.

1. Para a edificação da capacidade operacional de ciberdefesa na Marinha Portuguesa pode ser considerada a metodologia DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade).

Doutrina – Relaciona-se com "os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum" (Neves & Correia, 2016).

Organização – Permite a constituição dos "indivíduos em equipas, e estas em unidades operacionais, para a execução coordenada das funções (…) [de modo a] atingirem os objetivos operacionais da organização" (Neves, 2015).

Treino – Visa preparar os "diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais (…) sendo relevante as lições aprendidas através do treino" (Neves, 2015).

Material – Composto por "tudo o que é necessário para suportar e equipar as unidades operacionais (…) ou seja, todo o material que tenha relevância para o sucesso da missão" (Neves & Correia, 2016).

Liderança – Refere-se "à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar (…) [dirigindo e motivando] os membros da equipa, (…) sabendo aproveitar eficazmente as mais-valias dos vários elementos" (Neves & Correia, 2016).

Pessoal – Compete "à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas" e garantir que estes possuem as qualificações necessárias para o desempenho da missão (Neves & Correia, 2016).

Infraestruturas – "Disponibilização de instalações adequadas à preparação e condução das operações" (Neves & Correia, 2016).

[53] A presente entrevista foi proposta ao atual Coordenador do Núcleo CIRC da Marinha, Comandante Courela Alexandre, a exercer funções desde fevereiro de 2019, que optou por solicitar a colaboração do Comandante Baptista das Neves para resposta da mesma.

Interoperabilidade – Referente "à necessidade de interagir com parceiros externos, (…) que colaboram para atingir [o] mesmo objetivo" (Neves, 2015).

Com base nesta metodologia e sendo o foco deste estudo a Marinha Portuguesa, quais/qual o(s) aspeto(s) que considera ser(em) mais relevante(s) em cada domínio da referida metodologia?

Resposta:

Doutrina – Sendo esta dimensão dedicada aos "princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum", importa dizer que na verdade não existe formalmente nenhuma Doutrina aprovada na Marinha dedicada à Ciberdefesa. O que existe é um conjunto de publicações doutrinárias do EMA, os PCA, que foram escritos como documentos enquadradores da organização dos sistemas de informação (SICA), às comunicações e serviços na Intranet e Internet, e finalmente à edificação de uma capacidade de resposta a incidentes cibernéticos que afetem a segurança da informação.

Quando o tema é Ciberdefesa torna-se fundamental a existência de doutrina operacional para a utilização do Ciberespaço, até agora inexistente quer na Marinha quer nas Forças Armadas.

Organização – Considerando a necessidade de uma estrutura de pessoal com "indivíduos organizados em equipas para a execução coordenada das suas funções, de modo a atingirem os objetivos operacionais da organização", a Marinha tem utilizado a equipa do Núcleo CIRC para responder às suas necessidades de participação nas várias ações de Ciberdefesa que vêm surgindo, desde a participação em exercícios de natureza cibernética nacionais e estrangeiros, a ações de formação específica na área da Ciberdefesa.

A principal questão é que a natureza e missão do Núcleo CIRC tem estado muito centrada na defesa dos nossos sistemas de informação internos e periféricos, com uma vertente importante na área da monitorização e resposta a incidentes, tendo havido pouco investimento numa componente operacional mais ativa própria da Ciberdefesa, área onde o Comando Naval deveria ter uma participação mais ativa na coordenação e condução das operações cibernéticas.

Treino – Esta dimensão assume particular importância na "preparação dos diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais". Através do Núcleo CIRC a Marinha tem participado na condução e

organização de vários exercícios nacionais e estrangeiros que se configuram com uma excelente (única) oportunidade de treino. Destacam-se pela sua relevância a participação nos exercícios nacionais Lusitano e CiberPerseu, de âmbito nacional, envolvendo todos os ramos e o EMGFA. A nível internacional destacam-se a participação nos exercícios Contex/Phibex e *Swordfish*, sendo também de relevar a participação com o Centro de Ciberdefesa nos exercícios *Locked Shields* e *Cyber Coalition*, entre outros.

Material – Nesta dimensão podemos considerar que a Marinha tem à sua disposição "tudo o que é necessário para suportar e equipar as unidades operacionais", no entanto é necessário acautelar a necessidade de manter os sistemas atualizados, com níveis de desempenho elevados, condições fundamentais para garantir a operacionalidade da Ciberdefesa na Marinha.

Liderança – Existe a perceção que as nossas chefias ainda não estão suficientemente sensibilizadas para as questões da cibersegurança e ciberdefesa, nem do impacto devastador que um ataque neste vetor poderá ter na Marinha e o impacto que tal ataque poderá ter no cumprimento da missão da Marinha. Se considerarmos a "preparação das chefias para uma abordagem profissional da operação", ou mesmo na "competência profissional para comandar" ações cibernéticas, teremos de dizer que ainda existe um importante caminho a percorrer.

Pessoal – A capacidade para "identificar os elementos mais capazes para o desempenho das tarefas e garantir que estes possuem as qualificações necessárias para o desempenho da missão" tem sido uma das maiores dificuldades para a Marinha e é transversal às Forças Armadas. Para além da dificuldade de identificação dos ativos humanos, existem sérios problemas ao nível da formação que importam corrigir, para além de não existir a capacidade de atrair novos elementos para os quadros nesta área específica, tendo em conta os valores remuneratórios que a Marinha oferece. Existe uma enorme falta de formação técnica ao nível dos Administradores de Domínio de Utilizador e de Oficiais de Segurança do Domínio de Utilizador, responsáveis locais nas unidades pelas questões de Cibersegurança e Segurança da Informação.

Infraestruturas – À semelhança do Material, esta dimensão encontra-se razoavelmente bem implementada podendo afirmar-se que estão disponibilizadas "instalações adequadas à preparação e condução das operações", sendo apenas necessário garantir a sua sustentabilidade e manutenção.

Interoperabilidade – Esta dimensão tem sido assegurada de forma muito satisfatória através de uma relação de dependência funcional entre os Núcleos CIRC dos Ramos e o Centro de Ciberdefesa. Através da participação conjunta em vários exercícios Nacionais e Internacionais tem sido assegurada a interação "com parceiros externos, que colaboram para atingir o mesmo objetivo".

2. Quais/qual o(s) domínio(s) que considera mais relevante(s) e essenciais/essencial para a capacidade de ciberdefesa da Marinha e de que forma se destaca(m) dos restantes?

Resposta:

Tal como um navio começa a ser construído pelo seu cavername, também a capacidade de Ciberdefesa necessita de uma Doutrina que suporte, oriente e defina os objetivos que a Marinha pretende alcançar. A inexistência de Doutrina específica para a Ciberdefesa leva ao surgimento de equívocos dentro da Organização e a ações pouco eficientes e eficazes.

O Pessoal é talvez o ponto mais crítico. A falta de recursos qualificados aos vários níveis, operacional, tático e estratégico, compromete a sustentabilidade da capacidade a médio prazo. A escassez de recursos humanos leva à sobrecarga dos ativos existentes e à impossibilidade de executar corretamente todas as tarefas que lhes estão atribuídas.

3. O NCIRC tem a missão de garantir a segurança e a defesa do ciberespaço da Marinha, através da resposta a incidentes, entre outras competências.

De que forma considera ser o desempenho do NCIRC de acordo com o pretendido para garantir o cumprimento da sua missão? No caso de existirem, quais as limitações que sente determinarem o normal e correto desempenho das funções do Núcleo?

Resposta:

Esta questão está de certo modo respondida na anterior.

O Núcleo CIRC da Marinha encontra-se inserido na organização da DITIC, com a missão de monitorizar a infraestrutura tecnológica de redes e serviços da Marinha, garantindo não só a resposta a incidentes, mas também o desempenho de ações preventivas e de representar a Marinha nos vários *foruns* em que a Marinha participa.

Importa dizer também que alguns dos cargos principais do Núcleo CIRC, como por exemplo o Chefe do Núcleo e o Oficial Forense são objeto de acumulação interna com outros cargos de segurança da DITIC, levando por isso à necessidade de muitas vezes estes elementos não estarem disponíveis para as ações de Cibersegurança. Acresce a isto o facto de, nem todos os cargos estarem preenchidos, tendo como consequência a sobrecarga de tarefas para os elementos do Núcleo.

Como é apanágio dos nossos militares, todos têm feito um esforço meritório de modo a garantir que o Núcleo CIRC tenha sempre conseguido cumprir satisfatoriamente a sua missão.

Apêndice D – Entrevista ao Comandante Caldeira Carvalho (EMA)

O Comandante Caldeira Carvalho desempenha atualmente funções no Núcleo de Ciberdefesa e Tecnologias de Informação e Comunicações, no Estado-Maior da Armada, e integrou o GT-EMA.

1. Para a edificação da capacidade operacional de ciberdefesa na Marinha Portuguesa pode ser considerada a metodologia DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade).

Doutrina – Relaciona-se com "os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum" (Neves & Correia, 2016).

Organização – Permite a constituição dos "indivíduos em equipas, e estas em unidades operacionais, para a execução coordenada das funções (…) [de modo a] atingirem os objetivos operacionais da organização" (Neves, 2015).

Treino – Visa preparar os "diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais (…) sendo relevante as lições aprendidas através do treino" (Neves, 2015).

Material – Composto por "tudo o que é necessário para suportar e equipar as unidades operacionais (…) ou seja, todo o material que tenha relevância para o sucesso da missão" (Neves & Correia, 2016).

Liderança – Refere-se "à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar (…) [dirigindo e motivando] os membros da equipa, (…) sabendo aproveitar eficazmente as mais-valias dos vários elementos" (Neves & Correia, 2016).

Pessoal – Compete "à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas" e garantir que estes possuem as qualificações necessárias para o desempenho da missão (Neves & Correia, 2016).

Infraestruturas – "Disponibilização de instalações adequadas à preparação e condução das operações" (Neves & Correia, 2016).

Interoperabilidade – Referente "à necessidade de interagir com parceiros externos, (…) que colaboram para atingir [o] mesmo objetivo" (Neves, 2015).

Com base nesta metodologia e sendo o foco deste estudo a Marinha Portuguesa, quais/qual o(s) aspeto(s) que considera ser(em) mais relevante(s) em cada domínio da referida metodologia?

Resposta:

Esta metodologia é focada na edificação de capacidades identificando as lacunas e / ou capacidades e edificar para servir de suporte à capacidade que se quer edificar.

No caso do plano de reforço da capacidade de ciberdefesa da Marinha posso identificar os seguintes pontos mais relevante:

D – Atualização da doutrina e alinhar com o CCD e aliados

O – Guarnecer com os recursos humanos a organização já definida e estudar a operacionalização da estrutura. A questão de C2 em operações é fulcral para o funcionamento eficiente da capacidade.

T – A formação adequada dos recursos humanos é fundamental para a capacidade, sem recursos humanos certificados não temos capacidade.

M – Atualização do parque informático e verificação da resiliência e capacidade DDR da esquadra.

L – Consciencialização que a ciberdefesa não é um problema dos técnicos, mas sim uma vertente das operações.

P – Captação, definição de carreiras e retenção do pessoal, é o grande problema de todas as organizações neste domínio.

I – Nada de especial a referir.

I – Garantir a interoperabilidade com o CCD, aliados e CNCS é crítico.

2. Quais/qual o(s) domínio(s) que considera mais relevante(s) e essenciais/essencial para a capacidade de ciberdefesa da Marinha e de que forma se destaca(m) dos restantes?

Resposta:

Todos os domínios são todos relevantes para a edificação da capacidade de ciberdefesa, a nossa capacidade global é restringida ao domínio menos bem conseguido.

No entanto, na minha opinião, o que mais se destaca e é o mais preocupante será o vetor do pessoal. Existe uma grande oferta de trabalho no mundo civil, e todos os

técnicos com algum know-how são contratados com vencimentos que a Marinha, nem nenhum organismo público pode concorrer.

Para resolver esse problema temos de encontrar mecanismos adequados de atrair, formar, dar uma carreira motivante e reter esse pessoal.

A solução passará por a Marinha assumir que será uma plataforma de formação e treino dos futuros técnicos que mais cedo ou mais tarde sairão para o mundo civil. Não deverá tentar contrariar isso, pois é uma batalha perdida ao início, mas sim planear e usar isso a seu favor e a favor de Portugal.

3. Com base na sua experiência, especialmente na sua participação no Grupo de Trabalho para o Plano de Ação para o Reforço da Ciberdefesa da Marinha, questiono-o como considera que este ramo esteja preparado a nível da cibersegurança.

Julga que a Marinha possui as condições/requisitos necessários para garantir eficazmente a segurança do seu ciberespaço? Quais os fatores, no caso de existirem, que considera serem mais críticos neste âmbito?

Resposta:

Penso que a marinha, em termos de material de defesa e deteção, está bem apetrechada e pode facilmente fazer frente a um ciber-criminoso comum. Embora a mentalização e a disseminação de boas práticas na utilização do ciberespaço, para os utilizadores do domínio, terá de ser melhorada.

Contra um ator estatal, a Marinha e as FFAA têm ainda um longo caminho a percorrer para o fazer autonomamente, mas com a ajuda dos aliados já consegue assegurar um nível aceitável de defesa.

Os pontos mais críticos é a consciencialização para as boas práticas dos utilizadores de domínio da Marinha e a atualização dos equipamentos informáticos utilizados nos processos de trabalho do dia a dia na organização. Uma parte considerável do parque informático da rede de Marinha encontra-se muito desatualizado tendo assim vulnerabilidades críticas para cibersegurança do domínio.

4. Na sua opinião, que resultados trará para a Marinha o exposto no Plano de Ação para o Reforço da Ciberdefesa da Marinha? E quais são as principais medidas propostas que concorrem para um maior impacto na ciberdefesa deste ramo?

Resposta:

Irá reforçar a capacidade de ciberdefesa e cibersegurança da Marinha, mantendo a organização alinhada com o definido no CCD-EMGFA e com os aliados. Este plano visa colmatar as fragilidades encontradas e garantir a resiliência da organização no ciberespaço.

Todas as medidas propostas são importantes, pois versam os diversos domínios de edificação da capacidade. Sem os domínios convenientemente desenvolvidos a capacidade não existe ou não tem a eficácia requerida para cumprir com a sua missão.

Apêndice E – Entrevista ao Engenheiro Marques Prates (EMA)

O Engenheiro Marques Prates desempenha atualmente funções no Núcleo de Ciberdefesa e Tecnologias de Informação e Comunicações, no Estado-Maior da Armada, e integrou o GT-EMA.

1. Para a edificação da capacidade operacional de ciberdefesa na Marinha Portuguesa pode ser considerada a metodologia DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade).

Doutrina – Relaciona-se com "os princípios fundamentais que permitem a utilização coordenada dos diversos meios para atingir um objetivo comum" (Neves & Correia, 2016).

Organização – Permite a constituição dos "indivíduos em equipas, e estas em unidades operacionais, para a execução coordenada das funções (…) [de modo a] atingirem os objetivos operacionais da organização" (Neves, 2015).

Treino – Visa preparar os "diferentes intervenientes para uma resposta pronta e capaz às necessidades operacionais (…) sendo relevante as lições aprendidas através do treino" (Neves, 2015).

Material – Composto por "tudo o que é necessário para suportar e equipar as unidades operacionais (…) ou seja, todo o material que tenha relevância para o sucesso da missão" (Neves & Correia, 2016).

Liderança – Refere-se "à preparação das chefias para uma abordagem profissional da operação, ou seja, ao desenvolvimento da competência profissional para comandar (…) [dirigindo e motivando] os membros da equipa, (…) sabendo aproveitar eficazmente as mais-valias dos vários elementos" (Neves & Correia, 2016).

Pessoal – Compete "à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas" e garantir que estes possuem as qualificações necessárias para o desempenho da missão (Neves & Correia, 2016).

Infraestruturas – "Disponibilização de instalações adequadas à preparação e condução das operações" (Neves & Correia, 2016).

Interoperabilidade – Referente "à necessidade de interagir com parceiros externos, (…) que colaboram para atingir [o] mesmo objetivo" (Neves, 2015).

Com base nesta metodologia e sendo o foco deste estudo a Marinha Portuguesa, quais/qual o(s) aspeto(s) que considera ser(em) mais relevante(s) em cada domínio da referida metodologia?

Resposta:

Doutrina – A inteligibilidade dos princípios fundamentais e no imediato o seu perfeito alinhamento com os princípios a definir pelo EMGFA-Centro de Ciberdefesa (CCD).

Organização – O desenho de uma organização focada para a capacidade para a qual foi constituída, com autonomia funcional de todos os setores e capaz de colaborar e cooperar com órgão externos à Marinha A organização deve, ainda, permitir uma flexibilidade que lhe permita adotar geometrias varáveis, e.g. constituição de equipas multidisciplinares, de modo a atingir os objetivos operacionais definidos.

Treino – Garantir, na máxima extensão possível, a participação/integração em exercício nacionais e internacionais.

Material –Equipar e suportar a organização com material a par da atualidade, interoperável, compatível e relevante para a missão.

Liderança – Promover a participação das chefias em fóruns dedicados, com especial enfoque na estratégia e nos efeitos.

Pessoal – Recrutamento, retenção e identificação de elementos capazes e consequente adaptação orgânica, através de novos quadros e requisitos de progressão.

Infraestruturas – Flexibilização das atuais instalações de forma a permitir a preparação e condução de operações de forma descentralizada.

Interoperabilidade – Promover a participação consistente em exercícios externos, preferencialmente com equipas modulares, tendo em vista assegurar a transversalidade de procedimentos, de equipamentos e de serviços no universo da defesa e demais órgãos com responsabilidades na segurança do ciberespaço.

2. Quais/qual o(s) domínio(s) que considera mais relevante(s) e essenciais/essencial para a capacidade de ciberdefesa da Marinha e de que forma se destaca(m) dos restantes?

Resposta:

Todos os “domínios” são relevantes e, sobretudo, indissociáveis na edificação de uma capacidade, no caso, da capacidade de Ciberdefesa da Marinha Portuguesa.

Importa assim revisitar todos os "domínios" de forma a atestar a sua consistência e o seu contributo para uma capacidade sólida.

Atualmente considero que o menos relevante se situa ao nível das infraestruturas, todos os outros assumem, assim, relevância dado, sobretudo, à incontornável necessidade de alinhamento com o EMGFA-CCD, Defesa e restante estrutura de segurança do ciberespaço.

3. Com base na sua experiência, especialmente na sua participação no Grupo de Trabalho para o Plano de Ação para o Reforço da Ciberdefesa da Marinha, questiono-o como considera que este ramo esteja preparado a nível da cibersegurança.

Julga que a Marinha possui as condições/requisitos necessários para garantir eficazmente a segurança do seu ciberespaço? Quais os fatores, no caso de existirem, que considera serem mais críticos neste âmbito?

Resposta:

Excluindo a área ofensiva e de exploração do ciberespaço, perspetivada para o EMGFA-CCD, a Marinha possui as condições/requisitos necessários a uma ação eficiente de segurança do seu ciberespaço. A eficácia só poderia ser traduzida através de uma capacidade resiliente, atualmente fragilizada nos domínios anteriormente indicados como mais relevantes (Doutrina, Organização, Treino, Material, Liderança, Pessoal e Interoperabilidade), e, portanto, críticos.

4. Na sua opinião, que resultados trará para a Marinha o exposto no Plano de Ação para o Reforço da Ciberdefesa da Marinha? E quais são as principais medidas propostas que concorrem para um maior impacto na ciberdefesa deste ramo?

Resposta:

Numa primeira análise, ao ser efetuada uma abordagem estruturada à edificação de capacidades consegue-se, consequentemente, identificar lacunas e áreas de reforço na atual capacidade edificada. Este será o principal resultado do Plano de Ação.

Das medidas propostas, as principais (com maior impacto) são as identificadas nos domínios anteriormente indicados como os mais relevantes. No entanto, e na atual conjuntura, considero que as medidas com maior impacto acabam por ser as relacionadas com o pessoal, que se estendem para além do domínio do "Pessoal", e.g.

Treino, Organização, i.e., onde a existência de recursos humanos é essencial para o desenvolvimento das medidas.

Apêndice F – Entrevista ao Engenheiro Câmara de Assunção (CCD)

O Eng.º Câmara de Assunção desempenha atualmente funções no Centro de Ciberdefesa.

1. No Art. 30º do DL n.º 184/2014, de 29 de dezembro, é apresentado o seguinte:

"2 - A DIRCSI, no âmbito da ciberdefesa, tem por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas.

- A DIRCSI tem ainda por missão, no âmbito da cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação dos sistemas de informação do restante universo da defesa nacional."

Simultaneamente, a Lei n.º 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço, aplicando-se também às FFFAA.

Tendo em conta o seguinte:

"6 — A presente lei não se aplica:

a) Às redes e sistemas de informação diretamente relacionados com o comando e controlo do Estado-Maior-General das Forças Armadas e dos ramos das Forças Armadas;

b) Às redes e sistemas de informação que processem informação classificada."

Pode ser considerado uma sobreposição de competências aos poderes de autoridade da Autoridade Nacional de Cibersegurança sobre as redes e sistemas de informação da Defesa que não as de comando e controlo ou as que processem informação classificadas?

Resposta:

A lei nº 46/2018, Regime jurídico da segurança no ciberespaço não atribui à Autoridade Nacional de Cibersegurança sobre as redes das Forças Armadas, muito pelo contrário como bem diz no seu e-mail o art 2º alínea 6 exceciona as redes das Forças Armadas deste regime jurídico. Mas é importante ver mais uma vez que falamos de redes das FFAA, mais precisamente das redes diretamente relacionadas

com o comando e controlo das FFAA (que na nossa perceção são todas as redes dos ramos e EMGFA). Em teoria as redes do MDN não estão excecionadas deste regime jurídico pois não são redes de comando e controlo das FFAA.

Este regime jurídico estabelece um conjunto de obrigações a que as entidades estão obrigadas no relato e ação a tomar em caso de incidentes de segurança da informação, não tenho conhecimento que atribua qualquer competência sobre a gestão e desenvolvimento das redes dos organismos a que se destina. Desta forma não há qualquer sobreposição de competências entre as várias entidades.

2. Uma das competências da DIRCSI passa por definir os "sistemas de comando, controlo (...)"(a) do nr. 5, Art. 30.º). A DIRCSI define também estes sistemas para a Marinha? Ou é o próprio ramo responsável por o fazer?

Resposta:

No que respeita à sua última questão a DIRCSI tem competências em termos de CSI nos sistemas de comando e controlo que são operados pelo EMGFA, bem como em sistemas que sirvam de suporte à designada RFCM (Rede Fixa de Comunicações Militares) que serve todos os ramos. Os restantes sistemas que vivem dentro das redes e sistemas dos Ramos são da responsabilidade de cada um dos Ramos. A única área de direção técnica detida pela DIRCSI sobre os Ramos tem precisamente a ver com a Ciberdefesa, e essa autoridade encontra-se vertida na LOEMGFA Art. 30º alínea 6 a): "6 – A DIRCSI, no âmbito da ciberdefesa, prossegue também as seguintes atribuições: a) assumir a direção e coordenação da capacidade nacional de ciberdefesa;"

Apêndice G - Entrevista ao Tenente Castro Veloso (ETNA)

O Tenente Castro Veloso desempenha atualmente funções como Chefe do Gabinete de Sistemas de Informação na Escola de Tecnologias Navais.

Esta entrevista não se insere na introdução mencionada anteriormente relativa às restantes entrevistas, pelas questões realizadas serem fechadas e muito concretas ao assunto, não exprimindo, com exceção da última resposta, uma opinião do entrevistado.

1. Que cursos existem para praças, sargentos e oficiais?
Qual o seu tempo de duração e os módulos abordados?

Resposta:

O GSI no seu catálogo de cursos dispõe de dois módulos que se enquadram no conceito de *ciber awareness*.

Para praças ministrado no âmbito de PAFMI no curso de formação de praças designado de Conceitos Gerais de Cibersegurança com 14 tempos de formação, dos quais 2 tempos são práticos e 1 tempo destinado a visita de estudo ao núcleo CIRC da Marinha.

Para todo o universo de marinha (civis, militarizados, praças, sargentos e oficiais) no âmbito de PAFMII o curso AKS70, com 18 tempos de formação e que é muito semelhante ao curso referido no ponto 1, diferenciando-se pelo fato de abordar a doutrina de Marinha para a conceção e operação dos sistemas de informação.

2. A ETNA realiza algum tipo de ação de sensibilização, ou está unicamente incluído nos cursos de formação?

Resposta:

Atualmente não.

3. Existem cursos específicos (praças, sargentos e oficiais) para preparar os militares para a execução de funções neste domínio? Quais?

(Como por exemplo, para ADU - Administrador do Domínio de Utilizador, GODU - Gestor Operacional do DU e OSDU - Oficial de Segurança do DU, ou para quem ocupa cargos no Núcleo CIRC - DITIC).

Resposta:

O Gabinete de Sistemas de Informação pretende, a curto/médio prazo disponibilizar o curso para ADU - Administrador do Domínio de Utilizador, para o de GODU - Gestor Operacional do DU e OSDU - Oficial de Segurança do DU existe essa intenção, mas que para já não passa de intenção.

No que se refere a cursos específicos para quem ocupa cargos no Núcleo CIRC - DITIC, para já não existe essa intenção em por diversos fatores dos quais se destacam:

A formação em causa seria demasiado especifica;

O número potencial de formandos seria sempre residual considerando o atual quantitativo do NCIRC;

4. Está previsto alguma alteração do atual plano de formação?
(Existência de mais cursos/palestras, formação mais alargada à comunidade de utilizadores, etc).

Resposta:

O Gabinete de Sistemas de Informação está presentemente a aumentar a oferta formativa existente na área de sistemas de informação, no entanto, pese embora não seja do âmbito da questão convém fundamentar quais os constrangimentos impeditivos de uma maior oferta/criação de novos cursos, o numero de elementos qualificados e escasso em toda a Marinha e a ETNA não é exceção, elementos esses que na maior parte do tempo estão a assegurar a formação prevista ou a atualizar os seus conteúdos, que nesta área especifica tem um período de reapreciação por vezes anual, sobrando assim muito pouco tempo para a investigação e desenvolvimento (pelo menos sem apoio externo) de novos cursos.

Por outro lado, também de referir que neste momento temos uma academia Microsoft que visa a disponibilização dos conteúdos e momentos de avaliação desta academia aos alunos da ETNA. Esta formação será disponibilizada em breve para todos os RH da Marinha.

Apêndice H - Entrevista ao Comandante Pratas Quaresma (COMNAV)

O Comandante Pratas Quaresma exerce atualmente funções como chefe da Secção de Sistemas de Informação no Comando Naval.

1. Que tipo de funções exerce o COMNAV e quais as suas competências no âmbito da cibersegurança/ciberdefesa?

Resposta:

De acordo com o RI que anexo, esta seção de acordo com a alínea c) do seu art.º 66 (pág. 23) compreende a Subsecção de Ciberdefesa.

"A Seção de Sistemas de Informação ao nível ciber, tem as seguintes competências:

a. Coordenar as atividades de ciberdefesa no âmbito das operações navais, no âmbito das suas competências;

b. Planear e coordenar o treino das forças e unidades operacionais na área da ciberdefesa;"

2. Nos exercícios nacionais navais (INSTREX, CONTEX/PHIBEX, SWORDFISH) são conduzidas séries ao nível da cibersegurança. Quem assume a coordenação destas séries de ciber é a DITIC mas em estreita coordenação com o COMNAV. Nestas situações, qual é ao certo o papel do COMNAV?

Resposta:

O tema ciber considerado um dos mais mediáticos do momento, tem ainda um longo caminho a percorrer. Por um lado, ainda numa fase muito mas muito inicial por outro, junta-se a necessidade de afirmação das organizações ciber, por exemplo nos Estados-maiores, a constituição de Divisões ciber independentes das divisões de Comunicações e Sistemas de Informação (DIV6/J6).

Os exercícios que se realizam incidem essencialmente em jogos tipo Quiz onde se respondem a questionários sobre as ações a tomar em determinado tipo de incidentes, estas séries são jogadas com base num sistema de "Brown envelopes".

A coordenação é assumida pela Ditic, assumindo o Comando Naval um papel de mero observador. O nível de ambição deste tipo de séries não justifica um empenhamento diferente por parte do Comando Naval.

3. Ao nível da cibersegurança e dentro das competências do COMNAV, considera existir algum constrangimento limitador para a execução das suas funções?

Resposta:

Os constrangimentos são sempre muitos, uma unidade como o Comando Naval com um ACE enorme, tem de acautelar uma série de situações como sendo:

a. A segurança da informação no setor, nomeadamente nos navios. Os Sistemas de bordo são de uma complexidade enorme e na sua generalidade não foram planeados para fazem face a incidentes ciber.

b. Os recursos humanos são à imagem de toda a nossa Marinha, um dos nossos maiores constrangimentos.

Em suma, os constrangimentos são enormes no modelo de edificação dos sistemas de informação e comunicação/combate a bordo, o que torna muito difícil a implementação de políticas de segurança nos referidos;

Os recursos humanos são cada vez menos, o que implica uma acumulação de funcional e nestas situações gerem-se prioridades e normalmente a Ciber nunca é prioridade, pelo menos até agora…

Síntese conclusiva:

O Comando Naval tem produzido uma série de documentos internos que revelam uma grande preocupação com a temática. O Próprio Estado-maior da Armada tem vindo revelar uma preocupação enorme com o que à Ciber diz respeito, mas o caminho ainda é longo e tem de partir pela sensibilização de todos sobre as reais consequências deste tipo de incidentes.

Nos exercícios organizados pela Marinha-Comando Naval, as séries Ciber são essencialmente de sensibilização, num caso de um Contex-Phibex atualmente a decorrer, a atenção que damos do CTF443 a esta temática é praticamente residual e respondendo à tua questão do papel que o Comando Naval assume, neste momento a prioridade gere-se ao momento, e a Ciber aparece porque tem de aparecer!!

Anexos

Anexo A – Missão, Estrutura e Competências da DIRCSI e do CCD

O seguinte texto transcreve as partes mais relevantes, para o presente trabalho, do Decreto Regulamentar n.º 13/2015, de 31 de julho, que aprova a orgânica do Estado-Maior-General das Forças Armadas.

Direção de Comunicações e Sistemas de Informação

Artigo 40.º

Missão e estrutura

1 - A DIRCSI tem por missão planear, estudar, dirigir, coordenar e executar as atividades inerentes aos sistemas de informação e tecnologias de informação e comunicação necessários ao exercício do comando e controlo nas Forças Armadas.

2 - A DIRCSI, no âmbito da ciberdefesa, tem por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas.

3 - A DIRCSI tem ainda por missão, no âmbito da cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação do restante universo da defesa nacional.

4 - A DIRCSI tem a seguinte estrutura:

(…)

e) O Centro de Ciberdefesa (CCD);

(…)

Artigo 45.º

Centro de Ciberdefesa

1 - Ao CCD compete:

a) Assumir a direção e coordenação da capacidade nacional de ciberdefesa, nomeadamente:

i) Conduzir operações militares no ciberespaço;

ii) Garantir a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas;

iii) Elaborar e manter atualizada uma carta de situação do ciberespaço, no domínio das Forças Armadas;

iv) Promover projetos de investigação e desenvolvimento, no âmbito da ciberdefesa;

v) Contribuir para o plano de formação, treino e qualificação dos recursos humanos das Forças Armadas, no âmbito da ciberdefesa;

b) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a ciberdefesa, nomeadamente:

i) Assegurar a capacidade permanente de deteção, resposta e recuperação de ciberincidentes;

ii) Efetuar a análise forense de ciberincidentes;

c) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço, nomeadamente:

i) Contribuir para a elaboração de políticas de segurança no ciberespaço;

ii) Elaborar requisitos de segurança para dispositivos de proteção periférica no ciberespaço;

d) Contribuir para as operações de informação, na vertente Computer Network Operations;

e) Assegurar a coordenação e o trabalho colaborativo e integrado com os núcleos Computer Incident Response Capability (CIRC) dos ramos das Forças Armadas e do EMGFA;

f) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com o Centro Nacional de Cibersegurança e os CIRC nacionais e internacionais;

g) Elaborar e divulgar boletins de segurança com recomendações e contramedidas a implementar em resposta a ameaças emergentes, no âmbito da ciberdefesa;

h) Planear, propor e organizar um programa de exercícios para obtenção de treino;

i) Propor a participação na representação nacional nos organismos nacionais e internacionais, no âmbito da ciberdefesa;

j) Exercer a autoridade técnica no âmbito da ciberdefesa e da cibersegurança setorial da defesa nacional;

k) Reforçar o CCOM, com elementos nomeados em ordem de batalha, quer em operações, quer para a realização de exercícios e treinos, nos planos externo e interno.

2 - No âmbito da cibersegurança setorial da defesa nacional, compete ao CCD:

a) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a cibersegurança setorial da defesa nacional;

b) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço;

c) Assegurar a coordenação e o trabalho colaborativo e integrado com os CIRC do universo da defesa nacional;

d) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com os CIRC nacionais e internacionais, de forma articulada com as competências de coordenação da cooperação nacional e internacional do Centro Nacional de Cibersegurança;

e) Cooperar com as estruturas nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.

Anexo B – Estratégia Nacional de Segurança do Ciberespaço 1.0 (ENSC 1.0)

O seguinte texto é construído pela compilação de transcrições da ENSC 1.0, aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho.

1. A Estratégia (…) funda-se no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas.
2. A Estratégia (…) alicerça-se nos seguintes cinco pilares:
   a. Subsidariedade: A segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o funcionamento do Estado, para o desenvolvimento económico e a inovação, bem como para a confiança dos cidadãos no mercado digital e no ciberespaço.
   b. Complementaridade: A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, militares ou civis, coletivos ou individuais.
   c. Cooperação: (…) a segurança do ciberespaço requer uma forte cooperação e colaboração entre aliados e parceiros, nacionais e internacionais (…).
   d. Proporcionalidade: Os riscos inerentes ao ciberespaço devem ser avaliados e geridos de forma adequada, assegurando -se a proporcionalidade dos meios e medidas para o seu exercício.
   e. Sensibilização: A garantia da segurança das infraestruturas tecnológicas, das redes e dos sistemas de informação depende da capacidade de os utilizadores finais saberem tomar medidas que previnam os riscos a que se encontram expostos. A sensibilização constitui um eixo essencial à preservação da segurança no ciberespaço.
3. A Estratégia desenvolve -se nos seguintes objetivos estratégicos:
   a. Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
   b. Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;

c. Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais;
d. Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

4. As implicações e necessidades associadas a cada um dos objetivos estratégicos permite definir uma orientação geral e específica, traduzida em seis eixos de intervenção, enformados em medidas concretas e respetivas linhas de ação, destinadas a reforçar o potencial estratégico nacional no ciberespaço, a saber:

Eixo 1 — Estrutura de segurança do ciberespaço;
Eixo 2 — Combate ao cibercrime;
Eixo 3 — Proteção do ciberespaço e das infraestruturas;
Eixo 4 — Educação, sensibilização e prevenção;
Eixo 5 — Investigação e desenvolvimento;
Eixo 6 — Cooperação.

Eixo 1 — Estrutura de segurança do ciberespaço:
(…)
3) Desenvolver a capacidade de Ciberdefesa:

a. Concretizar a Orientação Política para a Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, de 11 de outubro, publicado no Diário da República n.º 208, 2.ª série, de 28 de outubro, edificando a estrutura de ciberdefesa nacional;
b. Estabelecer e consolidar uma estrutura de comando e controlo da ciberdefesa nacional, recaindo as atribuições de orientação estratégica -militar da ciberdefesa sobre o Conselho de Chefes de Estado -Maior (CCEM) e o planeamento e resposta imediata e efetiva a uma crise no ciberespaço ao Centro de Ciberdefesa (CCD) e às capacidades dos ramos das Forças Armadas;
c. Implementar, desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional;
d. Constituir a ciberdefesa uma área onde é necessário promover sinergias e potenciar o emprego dual das suas capacidades, no âmbito das operações militares

e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão.

Anexo C – Estratégia Nacional de Segurança do Ciberespaço 2.0 (ENSC 2.0)

O seguinte texto é construído pela compilação de transcrições da ENSC 2.0, aprovada pela RCM n.º 92/2019, de 5 de junho, e apresenta as linhas orientadores dirigidas às FFAA. São expostos igualmente alguns pontos que, embora não particularizem a sua aplicabilidade às FFAA, podem ser considerados como tal.

1 — Valores, definições e princípios

A presente Estratégia alicerça-se nos seguintes princípios:

Princípio da subsidiariedade:

[A] responsabilidade inicia -se no próprio indivíduo, pela forma responsável como utiliza o ciberespaço, e termina no Estado, enquanto garante da soberania e dos princípios constitucionais.

Princípio da complementaridade:

A segurança do ciberespaço é uma responsabilidade partilhada entre os diferentes atores (…).

Princípio da proporcionalidade:

(…) a adequação e a alocação de recursos deve ser proporcional aos riscos identificados e à execução das linhas de ação constantes da presente Estratégia.

4 — Objetivos estratégicos

Objetivo estratégico 1 — Maximizar a resiliência:

Fortalecer e garantir a resiliência digital nacional potenciando a inclusão e a colaboração em rede de forma a salvaguardar a segurança do ciberespaço de interesse nacional (…).

Objetivo estratégico 2 — Promover a inovação:

Fomentar e potenciar a capacidade nacional de inovação afirmando o ciberespaço como um domínio de desenvolvimento económico, social, cultural e de prosperidade.

Objetivo estratégico 3 — Gerar e garantir recursos:

Contribuir para obter e garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço.

5 — Eixos

Eixo 1 — Estrutura de segurança do ciberespaço;

Eixo 2 — Prevenção, educação e sensibilização;

Eixo 3 — Proteção do ciberespaço e das infraestruturas;

Eixo 4 — Resposta às ameaças e combate ao cibercrime;

Eixo 5 — Investigação, desenvolvimento e inovação;

Eixo 6 — Cooperação nacional e internacional

Eixo 1 — Estrutura de segurança do ciberespaço;

A complexidade e a abrangência dos desafios da segurança do ciberespaço requerem uma liderança e governação forte e transversal, uma coordenação operacional ágil, célere e eficaz, uma capacidade de resposta e salvaguarda dos interesses nacionais e, acima de tudo, uma envolvência de recursos, conhecimentos e competências.

Assim, no âmbito deste eixo devem ser adotadas as seguintes linhas de ação:

Reforçar a capacidade de ciberdefesa nacional tendo em vista maximizar a resiliência das Forças Armadas para fazer face a incidentes ou ciberataques significativos que afetem os interesses e a soberania nacionais, devendo ser utilizados todos os meios para responder a ciberataques, incluindo a capacidade ofensiva no ciberespaço, sendo fundamental uma estreita ligação e coordenação com os diversos atores relevantes em casos de incidentes;

Aprofundar o emprego dual das capacidades de ciberdefesa, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão;

Aplicar a legislação complementar ao regime jurídico de segurança do ciberespaço assegurando um enquadramento legal claro para todos, designadamente, em relação aos requisitos de segurança a cumprir, aos limiares para determinar o impacto de um incidente e aos requisitos de notificação de incidentes;

Reforçar o papel das comunidades das equipas de resposta a incidentes de segurança informática como plataforma de excelência para a resposta operacional coordenada e a partilha de boas práticas e de informação relativa a incidentes;

Eixo 2 — Prevenção, educação e sensibilização

Neste contexto, é fundamental informar, sensibilizar e consciencializar não só as entidades públicas, mas, também as empresas e a sociedade civil. Por outro lado, é fundamental que o país se dote de recursos humanos qualificados para lidar com os complexos desafios da segurança do ciberespaço.

Desta forma (…) devem ser adotadas as seguintes linhas de ação:

Reforçar os meios de recolha e processamento de informação e as capacidades de análise;

Antecipar a emergência, evolução e mutação das ameaças, possibilitando a adoção atempada de ações que acrescentem resiliência;

Promover programas de capacitação em cibersegurança, robustos e transversais a todas as organizações (…);

Garantir um nível elevado da qualidade dos cursos de formação e de requalificação em cibersegurança (…);

Criar mecanismos de retenção em entidades nacionais de recursos humanos qualificados no âmbito da segurança do ciberespaço;

Organizar e realizar exercícios que permitam avaliar o grau de preparação e a maturidade das diversas entidades para lidar com incidentes com impacto relevante, potenciando sinergias. Adicionalmente participar em exercícios de âmbito internacional;

Tirar proveito das estruturas de ensino e formação militares e policiais nacionais e internacionais, aproveitando em particular a oportunidade da edificação em Portugal de estruturas específicas de ensino da Organização do Tratado do Atlântico Norte e da União Europeia e iniciativas associadas (…);

Sensibilizar as entidades nacionais para as respetivas vulnerabilidades específicas, passíveis de serem infiltradas, exploradas ou subvertidas no campo digital por agentes de ameaça diversos.

Eixo 3 — Proteção do ciberespaço:

A segurança do ciberespaço é parte integrante da segurança nacional e é essencial para o regular funcionamento do Estado (…).

Assim, para o presente eixo devem ser adotadas as seguintes linhas de ação:

Promover o contínuo desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço (…);

Maximizar a segurança e a defesa das redes e sistemas de informação das Forças Armadas e da Defesa Nacional tendo em vista a manutenção da capacidade de operação no ciberespaço através da capacidade de ciberdefesa defensiva.

Eixo 4 — Resposta às ameaças e combate ao cibercrime:

(…) Passa pela capacitação das entidades responsáveis pela segurança do ciberespaço de mecanismos defensivos e de resposta (…) [para] uma ação apropriada.

(…) Uma resposta em rede potenciará e tornará resiliente o esforço e capacidade de toda a comunidade envolvida na mitigação dos riscos (…);

Assim, devem ser adotadas as seguintes linhas de ação:

Desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional;

Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas, tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço;

Consolidar e promover a capacidade nacional de conhecimento das ameaças à segurança do ciberespaço, de forma colaborativa entre as autoridades nacionais com responsabilidade nesta área (…);

Fomentar e incentivar a participação das equipas de resposta a incidentes de segurança informática nos *fora* nacionais e internacionais especializados em segurança do ciberespaço (…);

Eixo 5 — Investigação, desenvolvimento e inovação:

(…) Pretende -se fortalecer, apoiar e promover o potencial nacional de investigação, desenvolvimento e inovação de processos e tecnologias de vanguarda para a cibersegurança (…).

Assim, devem ser adotadas as seguintes linhas de ação:

Promover a produção científica, o desenvolvimento e a inovação nos vários domínios da segurança do ciberespaço (…);

Potenciar sinergias nacionais e atender aos esforços cooperativos em curso nas organizações internacionais de que Portugal faz parte integrante (…) para, em colaboração com as universidades, centros de investigação e a indústria, desenvolver soluções tecnológicas com interesse para duplo uso civil e militar;

Participar nos trabalhos das comissões técnicas nacionais e internacionais, para implementar as normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação

Eixo 6 — Cooperação nacional e internacional:

(…) A presente Estratégia preconiza um dever reforçado de cooperação entre as estruturas e entidades nacionais com responsabilidade nas áreas que contribuem para a segurança do ciberespaço (…).

Adicionalmente importa caracterizar a participação nacional nas diversas atividades de ciberdefesa no contexto internacional onde Portugal se insere (…).

Deste modo, no âmbito deste eixo devem ser adotadas as seguintes linhas de ação:

Participar nos exercícios de cibersegurança e de ciberdefesa reforçando e aumentando o nível de maturidade para a proteção do ciberespaço, onde a partilha de informação e conhecimento constitui um fator fundamental;

Integrar organismos internacionais de cibersegurança e de ciberdefesa tendo em vista a cooperação internacional e a afirmação de Portugal neste domínio;

Aprofundar a coordenação e cooperação entre as diversas entidades nacionais com responsabilidades na segurança do ciberespaço, tendo em vista uma melhor capacidade de alerta e resposta para fazer face às ameaças;

Anexo D – Organograma da DITIC

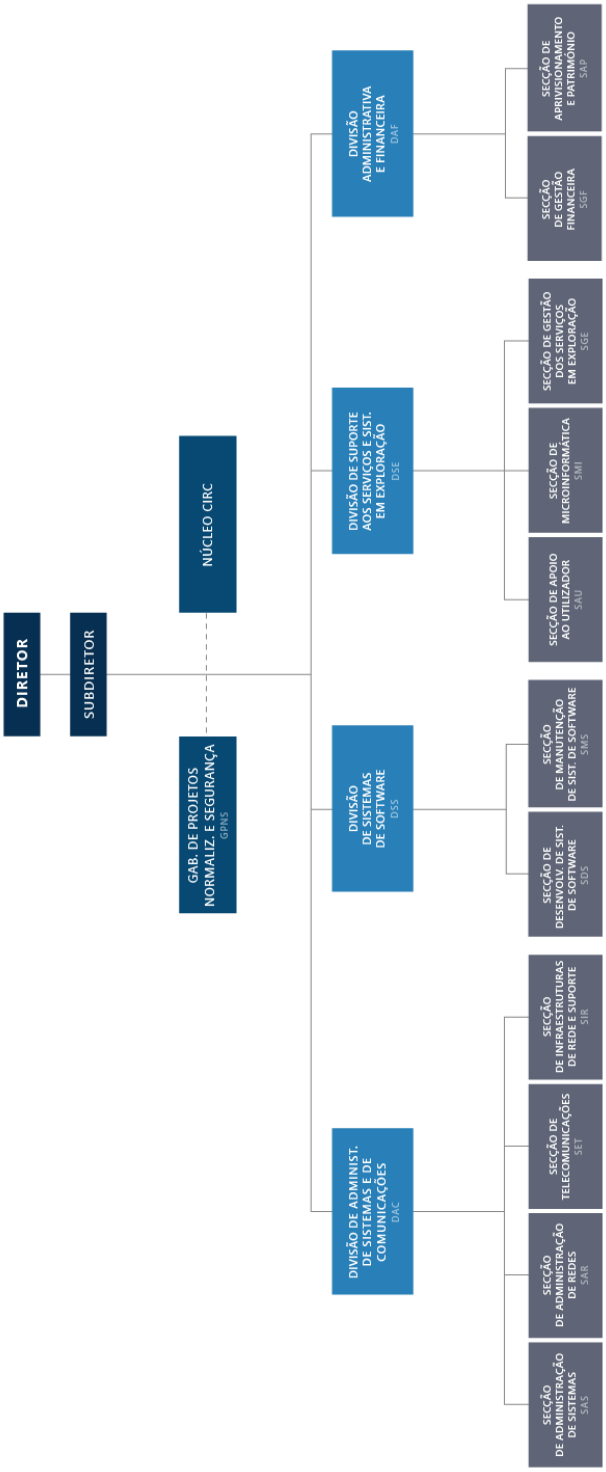

Figura 3 Organograma da DITIC

Fonte: DITIC-NCIRC, n.d.

Anexo E – Competências do Núcleo CIRC

O seguinte artigo é transcrito do Regulamento Interno da DITIC a que se refere o artigo único do Despacho do Almirante Chefe do Estado-Maior da Armada n.º 50/2016, de 10 de maio.

Regulamento Interno da Direção de Tecnologias de Informação e Comunicações

Artigo 10.°

Núcleo de Resposta a Incidentes de Segurança

1 - Ao Núcleo CIRC compete:

a) Garantir a capacidade de resposta a incidentes de segurança e defesa do ciberespaço e da informação de Marinha (Computer Incident Response Capability), através da operação, manutenção e monitorização avançada da estrutura e dos sistemas de segurança e controlo da informação;

b) Assegurar a coordenação técnica da resposta a incidentes de segurança da informação (*Computer Security Incident Response Team* - CSIRT), de forma transversal na Marinha, designadamente no apoio direto e de proximidade à componente operacional;

c) Assegurar a coordenação com o Centro de Ciberdefesa e com os Núcleos CIRC dos ramos na resposta a incidentes de segurança ao nível das Forças Armadas ou das infraestruturas críticas nacionais;

d) Planear, executar e coordenar as atividades de ciberdefesa e de gestão de crises no ciberespaço, no âmbito da segurança da informação e das comunicações de redes na Marinha, e em coordenação com o Centro de Ciberdefesa;

e) Participar no trabalho colaborativo e integrado com os restantes Núcleos CIRC que integram a capacidade de ciberdefesa nacional, incluindo a representação da Marinha em exercícios de natureza cibernética nacionais e internacionais;

f) Partilhar informação numa estratégia de proteção e resposta defensiva colaborativa com os Núcleos CIRC nacionais e internacionais, no âmbito das suas competências;

g) Assegurar, no âmbito das suas competências, a gestão e tratamento de incidentes de segurança da informação, fazer recolha de prova e realizar ações de investigação forense;

h) Desenvolver uma estratégia de comunicação com a comunidade de gestores e utilizadores dos sistemas de informação, através da manutenção de conteúdos e de recomendações de segurança e publicação de alertas e boletins informativos;

i) Colaborar para o conhecimento situacional do ciberespaço da Marinha e da defesa nacional.

2 - O Núcleo CIRC é reforçado por técnicos das diferentes áreas tecnológicas, durante a realização de exercícios na área da cibersegurança e ciberdefesa, nacionais e internacionais, e em situações de resposta a incidentes.

3 - A chefia do Núcleo CIRC é assegurada, em acumulação, por um oficial do GPNS, na direta dependência do Subdiretor de Tecnologias de Informação e Comunicações.