ESCOLA NAVAL

talant de bien faire

Cláudio Alexandre Colaço Cosme

Desenvolvimento do Conhecimento Situacional do Ciberespaço na Marinha/AMN e a sua contribuição no processo de tomada de decisão

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

Alfeite

2016

ESCOLA NAVAL

Cláudio Alexandre Colaço Cosme

Desenvolvimento do Conhecimento Situacional do Ciberespaço na Marinha/AMN e a sua contribuição no processo de tomada de decisão

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

Orientação de: CALM Gameiro Marques

Coorientação de: CFR EN-AEL Ribeiro Correia

O Aluno Mestrando

O Orientador

_____

_____

Alfeite

2016

DEDICATÓRIA

Aos meus familiares e amigos que
sempre me apoiaram em todas as minhas
decisões.

AGRADECIMENTOS

À minha Família, pelo apoio que prestou ao longo da realização deste estudo, ao meu Orientador e Co-orientador assim como às restantes entidades que me auxiliaram na elaboração deste trabalho.

RESUMO

Com a crescente dependência do ciberespaço, considerado o quinto domínio, é necessário que, para garantir a segurança dos sistemas de informação, as organizações civis como o Centro Nacional de Cibersegurança ou o Gabinete Nacional de Segurança e as organizações militares como o Estado-Maior General das Forças Armadas ou o Centro de Ciberdefesa, detenham um sólido conhecimento situacional do mesmo. Para alcançar este objetivo é fundamental que estas mesmas organizações colaborem de modo a desenvolver uma capacidade de prevenir e recuperar de ataques que possam ocorrer nesse domínio através de uma observação contínua do mesmo contribuindo, assim, para a sua proteção, prevenção, mitigação, resposta e para a sua recuperação. Deste modo, uma vez que os sistemas de informação são mais vulneráveis por estarem ligados em rede, apresentam potenciais riscos para as organizações pondo em causa a sua segurança. Por conseguinte, antecipar os eventuais problemas que poderão ocorrer nesses sistemas contribui para o desenvolvimento e implementação de medidas para proteger a informação. Sendo assim, e conforme outras organizações, também a Marinha está ligado em rede, pelo que está sujeita a este tipo de ameaça.

Com o presente trabalho, pretende-se abordar o tema do Conhecimento Situacional do Ciberespaço e mostrar a sua importância para o tema através da compreensão do modo como pode influenciar a condução das missões atribuídas às UN bem como as unidades em terra. Pretende-se identificar se existe uma organização a bordo das UN que, em articulação com comandos em terra, possa garantir que, num determinado teatro de operações, o que se passa no ciberespaço de interesse para a missão, tanto a nível tático como a nível operacional, é acionável. Pretende-se, ainda, em alinhamento com o conceito de capacidade caracterizar o que é que a Marinha tem desenvolvido neste contexto relativamente a doutrina, organização, estrutura, formação assim como treino.

PALAVRAS-CHAVE

Conhecimento Situacional do Ciberespaço, Capacidade, Cibersegurança, Ciberdefesa, Organização

ABSTRACT

Cyberspace is considered to be the fifth domain and nowadays every system and organization depend more and more on it. Therefore, it is essential to ensure that national civil and military organizations, such as Cybersecurity National Centre, National Security Agency, Cyber Defense Centre and Armed Forces General Senior Staff, have a solid situational knowledge of its respective cyberspace of interest. In order to achieve this objective it is important that these organizations cooperate among themselves to develop a capability which will allow them to prevent and recover from attacks that may occur in this domain at national level. This is possible through the continuous observation of the cyberspace which enables the contribution for the protection, prevention, mitigation, response and recovery from any attack that may occur. Since every system is connected through networks, their vulnerability increases, thus presenting a potential risk for the organizations, which may affect their own level of security. As a result, anticipating any issues that may occur in those systems contributes to the development and implementation of measures to proactively protect the most valuable information. The same occurs in the Portuguese Navy since this organization is also connected to its partners through networks. Therefore, it is also exposed to this new kind of threat.

The document addresses the concept of Cyberspace Situational Knowledge in order to demonstrate its importance, and to yield the understanding on how it may contribute to the successful completion of the missions assigned to naval units, as well as to the commands a shore. This study is also intended to identify whether there is on board an entity that, with the support of the on shore commands, is able to proactively contribute to the assigned missions as far as cyberspace matters are concerned. Moreover, the purpose of this work is to ascertain what the Portuguese Navy has relating doctrine, structure, organization, training and education with cyberspace, In accordance with the concept of capability and its components.

KEY-WORDS

Cyberspace Situational Knowledge, Capability, Cybersecurity, Cyberdefence, Organization

ÍNDICE

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS xiii

1. Introdução 1

1.1 Importância do Estudo 2

1.2 Delimitação 3

1.3 Objetivos do estudo 3

1.4 Questão central, questões derivadas e hipóteses 3

1.5 Metodologia 4

1.6 Estrutura do documento 4

2. Conhecimento Situacional do Ciberespaço 5

2.1 Enquadramento 5

2.2 Conceito de Ciberespaço, Cibersegurança e Ciberdefesa 6

2.3 Ciclo de Boyd (OODA Loop) e Conhecimento Situacional 11

3. OTAN e UE 16

3.1 Organização do Tratado do Atlântico Norte – OTAN 16

3.2 União Europeia – UE 21

3.3 Comparação entre OTAN e UE 28

4. Em Portugal e nos Ramos das Forças Armadas 29

4.1 A nível Nacional 29

4.2 Exército 33

4.3 Força Aérea 33

4.4 Marinha 34

5. Conclusões e Recomendações 42

LISTA BIBLIOGRÁFICA 48

GLOSSÁRIO 53

ÍNDICES DE FIGURAS

Figura 1 - Relação entre os conceitos: Cibersegurança e Ciberdefesa no contexto nacional 11
Figura 2 - Interação entre as COI 13
Figura 3 - Diretiva SRI (retirada da apresentação "Implementing The NIS Directive" realizada por Steve Purser a 14ABR16) 27
Figura 4 - Estrutura e Organização da CRISI (Retirado do PCA 16) 37
Figura 5 - Ciclo de Gestão de Incidentes (retirada do PCA 16) 38
Figura 6 - Fases Macro de Gestão de Incidentes (retirado do PCA 16) 39

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

ACT – *Allied Command Transformation*

AMN – Autoridade Marítima Nacional

CCDCM – Centro de Comunicações, de Dados e Cifra da Marinha

CCD COE – *Cooperative Cyber Defense Centre Of Excellence*

CDC – *Cyber Defense Committee*

CDMA – *Cyber Defense Management Authority*

CDMB – *Cyber Defense Management Board*

CE – Comissão Europeia

CERT – *Computer Emergency Response Team*

CFSP – *Common Foreign and Security Policy*

CNA – *Computer Network Attack*

CND – *Computer Network Defense*

CNE – *Computer Network Exploitation*

CNO – *Computer Network Operations*

CN – Comando Naval

COI – *Community of Interest*

COMPUSEC – *Computer Security*

COMSEC – *Communication Security*

CORE – Centro de Operações de Rede

CSA – *Cyber Situational Awareness*

CSC – Conhecimento Situacional do Ciberespaço

CSDP – *Common Security and Defence Policy*

CSIRT – *Computer Security Incident Response Team*

CSK – *Cyber Situational Knowledge*

DF – Direção de Formação

DG Connect – *Directorate General for Communications Networks, Content and Technology*

DN – Direção de Navios

DSP – *Digital Service Provider*

EC3 – *European Cyber Crime Center*

EU-ECS – *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*

EDA – *European Defence Agency*

EEAS – *European External Action Service*

EM – Estado-Membro

EMGFA – Estado-Maior General das Forças Armadas

ENISA – *European Network and Information Security Agency*

ENSC – Estratégia Nacional de Segurança do Ciberespaço

ETNA – Escola de Tecnologias Navais

EUROJUST – *Judicial Cooperation Unit*

EUROPOL – *European Police Office*

IA – *Information Assurance*

IDN – Instituto da Defesa Nacional

INFOSEC – *Information Security*

IOT – *Internet of Things*

ITU – *International Technology Union*

MISP – *Malware Information Sharing Platform*

MNCD2 – *Multinational Cyber Defense Capability Development*

MNCD E&T – *Multinational Cyber Defence Education and Training Project*

NAC – *North Atlantic Council*

NC3 – NATO C3 BOARD

NCIA – NATO *Communications and Information Agency*

NCIRC – NATO *Computer Incident Response Capability*

NDPP – NATO *Defense Planning Process*

NETSEC – *Network Security*

NICP – NATO *Industry Cyber Partnership*

NIS – *Network and Information System Directive*

NMA – NATO *Military Authorities*

NSWAN – *NATO Secret Wide Area Network*

OODA – *Observe, Orient, Decide and Act*

OTAN – Organização do Tratado do Atlântico Norte

PE – Parlamento Europeu

ROE – *Rules of Engagement*

RRT – *Rapid Reaction Team*

SP – Superintendência do Pessoal

STI – Superintendência de Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

1. Introdução

O Conhecimento Situacional do Ciberespaço (CSC) é um tema emergente e em expansão, pelo que é necessário desenvolver procedimentos para recolha de dados e políticas que permitam a análise e processamento de informação naquele âmbito. Estas ações são essenciais para dotar as entidades com mecanismos de apoio à tomada de decisão e com ferramentas que permitam responder ao perigo dos ciberataques, protegendo a informação relevante produzida, processada e armazenada nos sistemas de comunicações, e de comando e controlo da Marinha e da Autoridade Marítima Nacional (AMN).

A segurança dos sistemas de informação não é apenas da responsabilidade de quem os utiliza, mas também das entidades com quem a organização se relaciona. De igual forma, a segurança dos sistemas de informação da Marinha não deve ser planeada de forma isolada, mas em colaboração com as instituições públicas e privadas, com as organizações militares nacionais (EMGFA, Exército, Força Aérea, Guarda Nacional Republicana) e internacionais e com as organizações civis (Gabinete Nacional de Segurança, Centro Nacional de Cibersegurança). Este conjunto de relações melhora a capacidade de prevenir e recuperar de eventuais ataques, desenvolvendo um conjunto de capacidades de cibersegurança em rede com o objetivo de se alcançar uma efetiva prevenção, deteção e dissuasão.

Com a crescente dependência do ciberespaço, é necessário deter um sólido conhecimento situacional, através nomeadamente, da perceção do meio em que se opera e assim contribuir para a proteção, prevenção, mitigação, resposta e recuperação de forma eficaz de potenciais problemas que poderão ocorrer. Este facto é ainda mais relevante uma vez que os diversos sistemas, estando ligados em rede, são mais vulneráveis e apresentam riscos significativos para as organizações, bem como para a segurança nacional. Ao antecipar o que poderá acontecer a esses sistemas, os responsáveis poderão desenvolver medidas eficazes para proteger[1] a informação que lhes permite cumprir as suas missões (MITRE Corporation, [s.d]).

Neste âmbito, o conceito do CSC consiste, num modo geral, na criação do conhecimento do ciberespaço, por forma a prever, identificar e localizar situações

[1] Proteção – Ato de proteger ou ser protegido. Esta palavra, nesta temática, pode ter dois sentidos: proteção reativa (na medida de atuar ou proteger os sistemas de informação de acordo com as consequências de um ataque); proteção preventiva (na medida de atuar ou proteger os sistemas de informação antes que um eventual ataque ocorra).

relevantes, que permita a tomada de decisões atempada e pertinente, que por sua vez levem a que as ações subsequentes provoquem os efeitos desejados na medida dos interesses de quem as toma (MARQUES C. G., 2013, pp. 13-15)

No entanto, como se poderá construir o CSC de modo a tornar o processo de decisão e de ação efetivo, dado que o ciberespaço não possui fronteiras tangíveis e a informação que nele circula é, muitas vezes, da responsabilidade de outros atores que poderão estar sujeitos a outras normas jurisdicionais?

1.1 Importância do Estudo

A utilização do ciberespaço é um assunto emergente e transnacional, sendo considerado, nos dias de hoje, um "espaço virtual" ou o quinto ambiente (os outros são: terra, mar, ar e o espaço) onde se desenvolvem hoje em dia a grande maioria das atividades de carácter económico ou social, entre outras.

Tendo em conta que grande parte dos sistemas estão interligados devido à existência de redes (*Network components*), os diferentes governos demonstram esforços para defender as suas áreas de interesse. Contudo, para que tal aconteça, é necessário edificar um processo de construção do conhecimento situacional do ciberespaço para um melhor entendimento deste tipo de meio, uma vez que qualquer entidade, que recorra a estes sistemas, está vulnerável a uma ameaça proveniente deste mesmo "espaço virtual" (IDN, 2013, pp. 8-9). No entanto, não se trata apenas de se obter o CSC, mas também de saber se as diferentes organizações estão aptas, em termos de doutrina, procedimentos, organização, e até mesmo a nível de estruturas, para fazer face aos desafios suscitados por este ambiente.

Contudo, obter um conhecimento situacional do ciberespaço apenas é possível, atualmente, através da identificação e caracterização das ameaças, das vulnerabilidades dos diferentes sistemas e das redes existentes nas estruturas vitais de uma dada nação. Acresce, ainda, que, neste processo de construção do CSC, é essencial ter em consideração a componente humana, visto que é devido a esta que é possível caracterizar os utilizadores deste quinto ambiente.

1.2 Delimitação

Uma vez que o tema pode ser abordado de várias formas devido à sua abrangência, torna-se necessário delimitá-lo de modo a tornar mais objetiva a sua investigação bem como a respetiva análise. Neste contexto, pretende-se investigar a importância do desenvolvimento do CSC na Marinha/AMN, referindo quais os fatores necessários para que tal aconteça e quais as consequências para as entidades decorrentes da existência deste processo. Mais propriamente, pretende-se investigar o impacto que terá na tomada de decisões, tendo para isso em consideração o CSC nos três níveis (tático; operacional; estratégico). Além disto, considerando o desenvolvimento do CSC, pretende-se igualmente investigar se existe uma organização a bordo das Unidades Navais (UN) que, em articulação com os comandos em terra, possa influenciar, tanto ao nível tático como ao nível operacional, a tomada de decisões nas diversas missões. Posto isto, este trabalho irá debruçar-se no CSC a nível tático (UN) e a nível operacional (Comandos em terra) na Marinha/AMN.

1.3 Objetivos do estudo

Tal como foi referido anteriormente, também a Marinha/AMN recorre a sistemas que estão ligados em rede tanto a bordo das UN como nos Comandos em terra. Posto isto, em primeiro lugar pretende-se explicar em que consiste o CSC assim como mostrar a sua relevância, tendo em conta, neste caso, os interesses para a organização. Como as UN e os comandos em terra estão interligados é importante perceber em que medida o processo do CSC poderá influenciar a condução das missões atribuídas.

Seguidamente, pretende-se averiguar qual a doutrina, organização e procedimentos existente na OTAN e na UE assim como a existente na Marinha portuguesa com o intuito de reforçar, melhorar ou até mesmo adotar determinadas medidas ou procedimentos face ao que já existe a nível nacional.

1.4 Questão central, questões derivadas e hipóteses

Estando já os objetivos estabelecidos e o tema delimitado, a investigação desenvolve-se em torno da seguinte questão central:

"O que é necessário existir para que o CSC seja construído nas Unidades Navais e nos Comandos em terra de modo a, num contexto tático e operacional, respetivamente, poder contribuir, de forma atempada, para as tomadas de decisão?"

A resposta para esta questão irá compreender as seguintes questões derivadas:

QD1 – Em que consiste e para que serve o Conhecimento Situacional do Ciberespaço?

QD2 – O que é que a OTAN e a UE dispõem em termos de organização, doutrina, políticas e entidades no âmbito do ciberespaço?

QD3 – O que é que existe na Marinha Portuguesa, tanto a bordo das Unidades navais como nos Comandos em terra, sobre o CSC?

1.5 Metodologia

A metodologia seguida na elaboração do estudo baseou-se na consulta de diversa documentação e bibliografia alusiva à temática em apreço, recorrendo a livros e artigos. Acedeu-se, ainda, a documentação oficial disponibilizada em diversos *sites* que veiculam informação referente ao tema em estudo, designadamente do Instituto de Defesa Nacional (IDN), da MITRE Corporation, da OTAN, UE. Em complemento, efetuaram-se entrevistas seletivas e dirigidas a especialistas neste domínio.

Tendo estabelecido a questão central, as questões derivadas e as respetivas hipóteses, passaremos à sua verificação através do método hipotético-indutivo.

1.6 Estrutura do documento

O trabalho está organizado em cinco capítulos. A seguir à presente introdução, ir-se-á descrever em que consiste o Conhecimento Situacional do Ciberespaço, tendo como objetivo caracterizá-lo e compreendê-lo. No terceiro capítulo, procurar-se-á identificar o que existe a nível da OTAN e UE sobre esta matéria, recorrendo à análise de documentação relativa aos procedimentos, doutrina bem como quanto à organização em vigor. No quarto capítulo, recorrendo a documentação nacional, pretende-se identificar o que existe, em termos de organização, doutrina e procedimentos, nas UN e nos Comandos em terra, para, posteriormente, comparar com a informação obtida no capítulo anterior, com o intuito de apresentar, no quinto capítulo, as conclusões do

estudo através das quais visaremos responder à questão central e, assim, ao enunciado do trabalho de investigação.

2. Conhecimento Situacional do Ciberespaço

2.1 Enquadramento

Ao longo do tempo tem-se verificado uma elevada evolução tecnológica que permitiu que as sociedades mais desenvolvidas aproveitassem esta oportunidade para fomentar o seu crescimento económico e social. Contudo, é importante realçar que aquele crescimento foi acompanhado pelo desenvolvimento e adoção de novas Tecnologias de Informação e Comunicação (TIC), as quais, estando presentes em quase tudo o que se faz na sociedade, passaram a condicionar a nossa vida de uma forma inexorável.

Este tipo de tecnologias permite que os diversos sistemas de uma sociedade estejam ligados em rede através do ciberespaço. Tendo em conta que os diferentes utilizadores destes sistemas utilizam a informação simultaneamente, podem surgir tanto novas oportunidades como novas ameaças no ciberespaço de interesse, o que irá ter repercussões significativas no que toca à condução política e estratégica de um Estado (IDN, 2013, p. 5). Este problema tenderá a aumentar cada vez mais devido à elevada dependência das TIC da grande maioria dos processos existentes na sociedade e à consequente utilização frequente do ciberespaço.

Neste contexto, a utilização destes sistemas com fins maliciosos, através do ciberespaço poderá prejudicar os Estados e as sociedades. Como exemplo, temos os casos da Geórgia em 2008, da Estónia em 2007 e o do Kosovo em 1999 entre outros (GEERS, 2008, pp. 3-5). Estes ciber incidentes mostram que é necessário que cada Estado adote as medidas adequadas no sentido de garantir a utilização segura do ciberespaço, de modo a propiciar a livre utilização desse meio na justa medida dos interesses desse Estado. Essas medidas são essenciais para garantir a segurança e defesa de um Estado, mais propriamente a segurança cibernética, que pode ser decomposta essencialmente em dois domínios distintos mas complementares: a Cibersegurança e a Ciberdefesa (IDN, 2013, p. 8).

Assim, com a crescente dependência do funcionamento em rede e pelo facto da maioria dos novos dispositivos fazerem cada vez mais parte dessa rede, é difícil assegurar o desenvolvimento e o bem-estar das entidades que compõem a sociedade, sem primeiramente garantir a segurança e a proteção das infraestruturas, em particular as de natureza crítica, e dos serviços que são fundamentais para a vida em sociedade (IDN, 2013, p. 8). Estas infraestruturas veiculam informação valiosa que, por estarem em rede com outros sistemas, tornam-se particularmente vulneráveis, pelo que é necessário desenvolver conhecimento sobre o que se passa no ciberespaço de interesse dessas entidades, de modo a que seja possível antecipar situações que possam vir a comprometer a sua livre utilização, incluindo a recolha intempestiva de dados sem a prévia autorização do seu proprietário. Trata-se, assim, de desenvolver Conhecimento Situacional sobre o Ciberespaço (CSC) de interesse.

Neste capítulo pretende-se mostrar em que consiste o CSC e a sua relevância para que uma determinada organização possa não só garantir a segurança e defesa das referidas infraestruturas críticas e respetivos serviços, como também do seu ciberespaço de interesse. Sendo assim, começaremos por explicar três conceitos que se consideram fundamentais para caracterizar o CSC.

2.2 Conceito de Ciberespaço, Cibersegurança e Ciberdefesa

O mundo, tal como o conhecemos, poderá ser caracterizado por cinco domínios, a saber: Terra; Mar; Ar; Espaço e por último o Ciberespaço. Este domínio, além de ser relativamente recente, difere dos outros porque foi criado pelo Homem. Por esta razão, a doutrina existente em relação à sua utilização é exígua e complexa uma vez que, contrariamente aos domínios físicos, o ciberespaço não dispõe de fronteiras tangíveis e não existe uma entidade global que a regule. Sendo assim, o ciberespaço é, de acordo com o *Tallin Manual*, "*The environment formed by physical and non-physical components, characterized by the use of computers and electro-magnetic spectrum, to store, modify and exchange data using computer networks.*" (SCHMITT, 2013, p. 258). Isto é, o ciberespaço é um domínio composto por diversas camadas, onde se incluem a dos Utilizadores, a Lógica, a do Circuito e a Geográfica. A camada dos Utilizadores é aquela onde todos nós temos acesso ao ciberespaço, sendo da nossa responsabilidade a informação que é colocada e partilhada com os outros. A camada Lógica corresponde às

aplicações e protocolos que permitem comunicação entre os utilizadores e entre utilizadores e os sistemas de armazenamento e processamento de informação. A camada Circuito refere-se aos componentes físicos da arquitetura de rede que permite a ligação entre sistemas. Finalmente, a camada Geográfica é onde estão localizados os sistemas de comunicações e de armazenamento de informação, em que a aplicação de legislação e de proteção de dados depende da zona de implementação dos sistemas de informação.

Portanto, o "ciberespaço transpõe a vida real para um mundo virtual, com características únicas que impõem novas formas de interação e relacionamento" (REPÚBLICA PORTUGUESA, 2015, p. 3738). Posto isto, o ciberespaço é utilizado por todos e por tudo, permitindo, assim, proporcionar meios essenciais para o bem-estar das pessoas e das sociedades. Com o grande desenvolvimento do mundo digital em que tudo está conectado à internet (Internet das Coisas – "*Internet Of Things*" IOT), aquele facto ainda se torna mais relevante. Contudo, este domínio, se mal utilizado, pode servir, também, para a guerra e para o combate, pelo que as diferentes entidades sentem a necessidade e mostram intenção de também aí defenderem os seus interesses. De uma forma mais abrangente, dado que o ciberespaço é um conjunto de redes e sistemas que estão interligados entre si, é importante ter em conta as vulnerabilidades associadas ao seu uso, assim como as ameaças que poderão afetar esses mesmos sistemas e redes, como por exemplo, a componente humana, visto que são as pessoas os primordiais utilizadores deste domínio e também o seu elo mais fraco.

Uma vez que o ciberespaço é essencial para o funcionamento de uma sociedade, o aumento da necessidade de aceder permanentemente à informação, torna-se fundamental controlar os acessos não autorizados a informação privilegiada. Porém, o ciberespaço apresenta algumas características que poderão ser relevantes no que toca à segurança e defesa deste domínio. O ciberespaço caracteriza-se por ser dinâmico pois os sistemas que o compõem estão constantemente a sofrer alterações devido à descoberta de novas vulnerabilidades, bem como o aparecimento de novos tipos de ameaças; o seu acesso apresenta um custo muito reduzido; detém grande capacidade de armazenamento e de processamento de grandes quantidades de informação; apresenta um carácter assimétrico porque neste domínio se podem provocar ações de grande impacto com relativamente poucos recursos; providencia um elevado nível de anonimato uma vez que é relativamente difícil detetar a origem do ataque; apresenta, além de um enorme crescimento (funcionalidades e velocidade da troca de informação), uma capacidade

para produzir efeitos físicos (dispositivos, estruturas); por último, o ciberespaço é transversal, isto é, pode afetar outras atividades essenciais para o bem-estar da sociedade (segurança e defesa dos Estados) tal como foi referido anteriormente (IDN, 2013, p. 10).

Antes de passarmos a explicar os conceitos de Cibersegurança e de Ciberdefesa, é necessário compreendermos o que é a Segurança da Informação (INFOSEC – *Information Security*). A garantia da informação (*Information Assurance* - IA) inclui a segurança física (como a segurança do pessoal e do material) e a segurança da informação (COMSEC; COMPUSEC; NETSEC) e é definida como a proteção e defesa dos sistemas de informação e da própria informação garantindo, assim, a sua disponibilidade, a sua integridade, a sua autenticação, a sua confidencialidade e o não-repúdio (NSA, 2011, pp. 1-4, 1-5). O conceito de INFOSEC, sendo mais restrito que a IA, é definido como a aplicação de medidas de segurança que visam a proteção de informação processada, armazenada ou transmitida através dos sistemas de comunicação e informação e também de outros sistemas eletrónicos, de modo a evitar a perda de confidencialidade, integridade ou disponibilidade, seja acidental ou intencional (NATO, [s.d], pp. V-A-4). Ou seja, de uma forma geral, a INFOSEC consiste na defesa dos sistemas de informação e telecomunicações com recurso a medidas e procedimentos essenciais para a proteção e a preservação da informação de modo a manter essas características (podendo também incluir serviços de autenticação, não-repúdio e rastreabilidade) (IDN, 2013, p. 11).

Um outro conceito fundamental que importa definir para a segurança de informação no ciberespaço é o de Cibersegurança. Conforme a organização *International Technology Union* (ITU) a Cibersegurança é o conjunto de ferramentas, de políticas, de conceitos, de orientações, de processos de gestão de risco, de ações, de atividades de treino e prática que, juntamente com as tecnologias, podem ser utilizados para proteger o ciberespaço bem como a organização e os seus meios. Nestes meios presentes na organização estão incluídos os sistemas computacionais, o pessoal, a infraestrutura, os serviços, os sistemas de telecomunicações e toda a informação transmitida e/ou armazenada através do ciberespaço. Isto é, a cibersegurança garante a consecução e a manutenção das propriedades de segurança da organização e dos seus meios contra ameaças relevantes no ciberespaço (ITU-T, 2008, pp. 2-3).

Para garantir a segurança da informação (INFOSEC), uma determinada organização recorre a uma equipa técnica designada por *Computer Emergency Response Team* (CERT). Esta equipa é responsável por definir os constituintes para responder aos ciberincidentes, ou seja, fornece os serviços necessários para lidar com os incidentes e para sustentar a recuperação das componentes dos sistemas quando ocorrem violações à segurança dos computadores (COMPUSEC). Muitos dos CERTs providenciam, igualmente, serviços educacionais e preventivos, de modo a mitigar os riscos e minimizar o número de respostas aos ciberincidentes (ENISA, [s.d], p. 10). No entanto, o ciberespaço, sendo o quinto domínio, também pode servir para a guerra e para o combate, tal como foi referido previamente, pelo que podem vir a ser realizadas, neste ambiente, operações militares específicas. É, assim, importante que exista ou que se implemente uma Cultura de Segurança, que permita assegurar a segurança de informação sensível pelo que, para que tal aconteça, é necessário considerar três aspetos: as pessoas; os processos e a tecnologia. Todos estes aspetos contribuem para a criação de uma Cultura de Segurança numa organização.

Relativamente ao conceito de Ciberdefesa, este está definido como o conjunto de medidas necessárias para a proteção dos componentes das infraestruturas TIC contra ciberataques (podendo estes serem ataques físicos ou não, com a intenção de perturbar os sistemas de informação de uma entidade) (IDN, 2013, p. 11). Ou seja, de acordo com a *Austrian Cyber Security Strategy* o conceito de ciberdefesa é definido como todas as medidas necessárias à defesa do ciberespaço através de meios militares apropriados para atingir os objetivos estratégicos militares. A ciberdefesa é um sistema integrado, comprometendo a implementação de todas as medidas relacionadas com as TIC e segurança de informação (Republic of Austria, 2013, p. 21).

Isto é, "A capacidade de ciberdefesa deve ser estruturada e desenvolvida de forma a prevenir e retardar a rápida progressão dos ciberataques, garantindo a sua deteção antecipada" (Despacho nº 13692/2013, 28 de outubro do MDN) através da implementação de medidas e ferramentas de vigilância assim como de um alerta avançado de modo a limitar os eventuais danos que os ciberataques poderão causar.

Tal como foi mencionado anteriormente, o ciberespaço, sendo um domínio moderno de guerra, é cada vez mais utilizado para operações militares. Assim, o conceito de ciberdefesa está relacionado com as operações efetuadas no ciberespaço (*Computer Network Operations* - CNO) incluindo "ações de natureza defensivas, de

exploração das capacidades dos possíveis adversários ou mesmo de reposta ofensiva" (IDN, 2013, p. 12). Neste contexto é relevante mencionar quais as capacidades das CNO para uma melhor compreensão do que se trata neste tipo de operações, que estão relacionadas com a ciberdefesa:

- *Computer Network Defense* (CND): medidas adotadas para "proteger, controlar, analisar, detetar e responder a atividades não autorizadas nos sistemas de informação e comunicações." (IDN, 2013, p. 12), recorrendo às redes de computadores. Contudo, este conjunto de medidas não se limita exclusivamente à proteção dos sistemas aliados de um adversário comum, pode também contemplar ações que visam explorá-lo a partir da própria organização.
- *Computer Network Exploitation* (CNE): através da utilização de redes de computadores é recolhida informação e dados sobre os sistemas de comunicações e de informação de um dado adversário (IDN, 2013, p. 12).
- *Computer Network Attack* (CNA): também é através da utilização das redes de computadores que se tomam determinadas ações para "interromper, negar, degradar ou destruir a informação tratada" pelos sistemas de informação e de comunicações, tanto do possível inimigo como dos próprios sistemas amigos (IDN, 2013, p. 12).

Estas capacidades das CNO são importantes para garantir a ciberdefesa de uma entidade e do seu ciberespaço de interesse

Os dois conceitos explanados (cibersegurança e ciberdefesa) são essenciais para uma determinada entidade garantir a segurança de informação (INFOSEC) bem como a segurança e defesa do seu ciberespaço de interesse contra diversas ciberameaças. A figura seguinte (IDN, 2013) representa a forma como os conceitos se relacionam.

Figura 1 - Relação entre os conceitos: Cibersegurança e Ciberdefesa no contexto nacional

2.3 Ciclo de Boyd (OODA Loop) e Conhecimento Situacional

Estando definidos os conceitos de ciberespaço, de cibersegurança e de ciberdefesa, essenciais para a compreensão do que se pretende explicar neste capítulo, também será útil aplicar o Ciclo de Boyd (RICHARDS, 2012) ao Conhecimento Situacional para um melhor entendimento desta matéria, sendo este conceito definido posteriormente.

Assim, a construção do CSC necessita de se balizar num processo no qual, através da partilha de informação e da construção de laços de confiança entre as pessoas que constituem a Comunidade de Interesse (*Community Of Interest* - COI), se desenvolve saber sobre o que se passa no ciberespaço de relevância para aquela comunidade.

Para melhor se explicar este processo é fundamental compreender-se o Ciclo de Boyd, que consiste num ciclo de quatro fases (*OODA Loop*), a saber: O – *Observe*, O – *Orient*, D – *Decide*, A – *Act*. Este ciclo é essencial para que as organizações desenhem uma estratégia eficiente para fazer face a ciberincidentes.

Assim, aplicando o Ciclo de Boyd, tem que primeiramente se "Observar" o ciberespaço de interesse. Esta etapa corresponde à tomada de consciência das organizações que fazem parte da COI relativamente ao que se passa no ciberespaço (envolve as dimensões física e virtual). Esta etapa do ciclo corresponde a uma fase de

vigilância (construção de um panorama). Seguidamente vem a etapa "Orientar" a qual recorre às componentes de análise, de correlação e de fusão da informação proveniente de várias fontes que operam no ciberespaço de interesse. Nesta fase do Ciclo de Boyd toda a informação obtida é analisada, correlacionada e fundida e por último, tendo em conta a partilha de informação entre os utilizadores das organizações pertencentes a uma determinada COI, é partilhada através da rede. Assim, considerando a capacidade cognitiva da dimensão humana, será possível a criação do necessário conhecimento situacional que posteriormente viabilize uma atempada tomada de decisões (corresponde à terceira etapa do Ciclo de Boyd – "Decidir"). Estas duas etapas correspondem a uma fase de comando, controlo e coordenação, ou seja, ao desenvolvimento do conhecimento situacional. Por último, segue-se a etapa final do Ciclo de Boyd que é "Atuar", durante a qual as organizações agem desejavelmente de forma antecipada e coordenada, consoante o conhecimento situacional de que dispõem, recorrendo às ferramentas disponibilizadas pelos sistemas TIC. Desta forma, contribuem para a modificação da situação no ciberespaço (MARQUES G., 2013, pp. 13-15). Este ciclo prossegue recorrentemente, permitindo, assim, a criação de conhecimento que viabiliza a ação subsequente de forma adaptativa à nova envolvente. Embora seja importante que cada entidade pertencente a uma COI utilize o Ciclo de Boyd como conceito enquadrador do processo, é ainda mais relevante se todas as entidades pertencentes às diferentes COI o utilizem e que posteriormente partilhem os resultados obtidos entre si para que se obtenha um cenário ainda mais completo do que se passa no ciberespaço de interesse (Figura 2). Para que tal aconteça é fundamental existir interoperabilidade[2] entre entidades e confiança entre COI's.

[2] De acordo com o AAP-6, interoperabilidade é: "The ability to operate in synergy in the execution of assigned tasks." – Capacidade de atuar/operar em conjunto na execução das tarefas atribuídas (NSA, 2008, pp. 24-8).

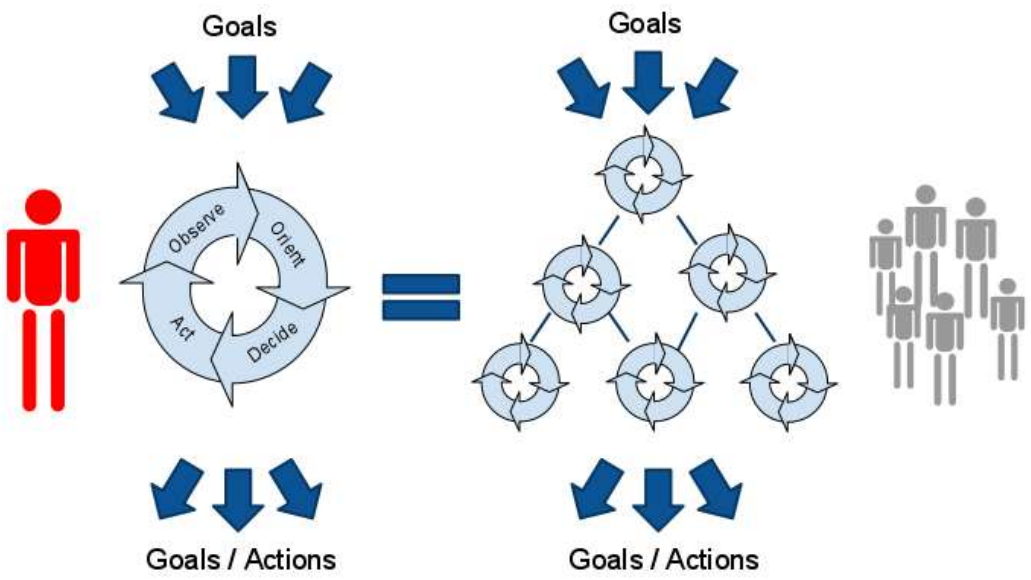

Figura 2 - Interação entre as COI

Após a explicação das quatro fases do ciclo de Boyd e tendo em consideração os conceitos já definidos de cibersegurança e de ciberdefesa, pode-se constatar que o recurso a este ciclo é útil e adequado para a edificação da capacidade de cibersegurança assim como para a de ciberdefesa. Isto porque tanto na cibersegurança como na ciberdefesa se realizam as quatro fases do ciclo para uma melhor solução dos problemas existentes. Nas duas primeiras (observação e orientação) recolhe-se toda a informação possível sobre as possíveis ameaças, sendo esta, posteriormente, processada, armazenada e correlacionada de modo a auxiliar na tomada de decisões e depois na ação. Porém, consoante se trate de cibersegurança ou de ciberdefesa, existem diferenças nestas duas últimas fases do ciclo (decisão e ação). De facto, como foi referido anteriormente, a capacidade de ciberdefesa é utilizada para desenvolver operações militares específicas (CNO), podendo um determinado Estado, além de desempenhar missões dentro do seu ciberespaço de interesse, atuar no ciberespaço do outro, de modo a defender os seus interesses ou até mesmo explorar as capacidades do adversário em benefício próprio. Por outras palavras, a "ação" no contexto da Ciberdefesa pode implicar atividades intrusivas no ciberespaço de interesse do adversário.

Refira-se que, para que tal aconteça, é necessária a existência de um enquadramento legal adequado, o qual, no contexto das operações em geral e das CNO's em particular, se deverá consubstanciar na produção de regras de empenhamento ou ROE's (*Rules Of Engagement)*.

Para melhor se compreender em que consiste o CSC, é essencial realçar a diferença entre *Cyber Situational Awareness* (CSA) e *Cyber Situational Knowledge* (CSK), este último corresponde ao CSC. O primeiro conceito (CSA) consiste na reação aos diversos eventos que tenham ocorrido, isto é, consoante os acontecimentos as organizações tomam medidas para tentar resolver estas situações. De forma genérica permite às organizações estarem cientes do que está a ocorrer e reagir em conformidade. Para isso têm em consideração toda a informação recolhida através da partilha de informação entre as organizações e também através de todos os sistemas. O CSC (CSK) consiste em providenciar as organizações com respostas atempadas e mais fundamentadas, ou seja, permite obter o conhecimento de modo a poderem prever e assim atuar de forma antecipada e coordenada a determinados eventos. Nesta situação é necessário considerar as componentes de análise, de correlação de dados adquiridos (informação proveniente dos sistemas TIC) e de fusão dos mesmos. Isto é possível se, para a criação destas componentes, se considerar o conhecimento adquirido através da existência de um determinado nível de confiança e de várias interações entre os utilizadores de uma COI (MARQUES G., 2013, pp. 13-15).

Para que tal seja possível é necessária a existência de processos eficazes, tecnologia apropriada e pessoal treinado e apto para atuar consoante os diversos eventos. Contudo, este último fator poderá pôr em risco uma organização (considerado o "elo mais fraco"), caso o pessoal não esteja ciente da relevância das funções que desempenha, bem como as consequências que certas das suas ações poderão causar, pelo que é fundamental que se implemente uma Cultura de Segurança na organização (MARQUES C. G., 2013, pp. 13-15). Neste contexto, afigura-se que as questões relacionadas com o CSC deverão ser enquadradas numa lógica de "*Capability*", de modo a colmatar as eventuais vulnerabilidades desses componentes e tornar a cultura de segurança eficaz e eficiente.

Posto isto, começaremos por definir o conceito de capacidade (*capability*). A capacidade é: "a habilidade para produzir um efeito que é necessário atingir. O efeito é o resultado de uma acção ou conjunto de acções produzidas pela capacidade. Uma capacidade consistirá numa ou mais componentes funcionais: Doutrina, Organização, Treino, Material, Liderança, Pessoal, Facilidades (infra-estruturas) e Interoperabilidade." (MADEIRA, 2008, p. 65).

Esta abordagem é útil para a edificação do CSC e para a implementação da Cultura de Segurança uma vez que garante um tratamento holístico do tema, viabilizando que todas as componentes que contribuem para a respetiva resolução sejam contempladas harmoniosamente. Assim, para que uma dada organização crie uma capacidade de CSC, deverá: (i) definir a Doutrina ("como fazer") necessária ao enquadramento do assunto; (ii) estabelecer a Organização e a Liderança adequada a que a capacidade se construa e se desenvolva; (iii) garantir o recrutamento e a formação (T) do Pessoal necessário; (iv) obter os sistemas (M) apropriados para o propósito em vista; (v) identificar as Infraestruturas necessárias ao funcionamento e operação dos sistemas, garantindo que o conjunto (Pessoas e Sistemas) sejam Interoperáveis com as COI em geral. Só assim se poderá definir e implementar políticas (o que fazer) e procedimentos de segurança, tornando-se possível controlar e influenciar o comportamento e ações do pessoal e dos sistemas de informação. Portanto, tal como foi mencionado anteriormente, o fator humano, sendo o mais frágil mas ao mesmo tempo o mais importante na tomada de decisões, leva a que a organização tenha que procurar incutir no seu pessoal um sentido de responsabilidade aquando do manuseamento de informação através de uma consciencialização efetiva da importância do que está em jogo. Para que tal seja possível é necessário, por um lado garantir que o pessoal tenha acesso a sólida formação na área em questão e por outro que esse pessoal tenha uma maior permanência em funções ligadas à cibersegurança e/ou ciberdefesa, atenta a complexidade dos respetivos temas. Esta permanência contribui, ainda, para o estabelecimento dos necessários laços de confiança entre as diversas entidades que constituem a COI os quais, em última instância, facilitam a partilha de informação nessa comunidade. A organização assume, assim, a responsabilidade por mostrar a importância do papel das pessoas em todos os processos atinentes (ex.: como reagir a incidentes de segurança; conhecer os processos básicos de segurança) e as consequências que as suas ações têm e a função das medidas de segurança, incluindo a razão da sua existência, pois isto tudo afetará o desempenho da organização (NEVES, 2014, pp. 272-273). Só assim se mitigam possíveis ações que se poderão transformar numa vulnerabilidade para a organização.

Contudo, também é fundamental que exista tecnologia apropriada. Esta tecnologia permitirá definir o modo como o pessoal deverá atuar na utilização dos sistemas de informação. Assim, conclui-se que o CSC permite às organizações preverem eventuais incidentes, uma vez que os dados obtidos, através de processos de

partilha no seio da COI, são analisados, correlacionados e fundidos, transformando-se em informação relevante para essa comunidade e viabilizando a obtenção de conhecimento do que está a ocorrer. Deste modo possibilita-se que essas organizações desenvolvam respostas atempadas e fundamentadas para que possam atuar, de forma oportuna e coordenada e assim fazer face a ciber incidentes. Portanto, face ao que antecede, consideramos que a questão derivada QD1 *"Em que consiste e para que serve o Conhecimento Situacional do Ciberespaço?"* se encontra respondida.

3. OTAN e UE

Neste capítulo pretende-se dar a conhecer o que existe na OTAN e na UE a nível de doutrina, procedimentos, medidas e organização interna assim como o que estas organizações pretendem fazer no futuro relativamente ao que se passa ou o que aconteceu no respetivo ciberespaço de interesse.

3.1 Organização do Tratado do Atlântico Norte – OTAN

A missão formulada da OTAN no ciberespaço tem como objetivo proteger as suas próprias Redes, aumentar as capacidades cibernéticas dos estados-membros e cooperar com as nações aliadas, com a UE e com as indústrias. Esta missão foi enunciada devido aos ciberataques de 1999 (ciber incidentes contra a OTAN e membros governamentais) durante a Operação "Allied Force" (HEALEY & JORDAN, 2014, p. 1). A OTAN efetuou a referida missão considerando as seguintes tarefas como essenciais para o cumprimento da mesma: a defesa coletiva e a dissuasão; a gestão de situações críticas e a segurança cooperativa através da existência de parcerias. Contudo, estas tarefas, consideradas primárias, englobaram não só a segurança dos estados-membros como também a proteção das organizações, das infraestruturas e das operações contra os ciberataques desses estados (PERNIK, 2014, p. 1).

Em 2002, a OTAN, na Cimeira em Praga, adotou um programa de Ciberdefesa como uma resposta parcial aos ciberataques ocorridos, tendo surgido deste programa uma entidade fundamental denominada NATO *Computer Incident Response Capability* (NCIRC), com a finalidade de prevenir, detetar e responder aos ciber incidentes

praticados contra os interesses da Aliança Atlântica (HEALEY & JORDAN, 2014, p. 1). Esta equipa especializada, bem como o programa de ciberdefesa, foram aprovados pelo *North Atlantic Council* (NAC). Esta entidade supervisiona os aspetos políticos na implementação e exerce funções de autoridade sobre a tomada de decisões relativas à gestão de situações de crise cibernéticas (PERNIK, 2014, p. 4).

Na sequência dos ciberataques perpetrados quer contra a Estónia em 2007, quer contra as páginas eletrónicas da Geórgia, em 2008, durante a guerra contra a Rússia, foi possível à OTAN perceber a envolvente do ciberespaço (PERNIK, 2014, p. 4). De facto, estes conflitos levaram a que a OTAN compreendesse realmente as implicações que estes tipos de ataques têm ao nível político, assim como a respetiva dimensão técnica. Assim, foi desenvolvida a primeira Política de Ciberdefesa da OTAN, aprovada na Cimeira de Bucareste, em 2008, na qual se referiu a necessidade da Aliança Atlântica e dos seus aliados possuírem uma capacidade de proteger os sistemas de informação vitais à respetiva soberania; de partilhar as melhores formas de atuação; e de providenciar às nações amigas a capacidade de auxiliar, quando requisitado, no combate aos ciberataques. Nesta sequência, e para ajudar a implementação dos objetivos definidos na Política de Ciberdefesa, criaram-se os seguintes organismos: *Cyber Defense Management Authority* (CDMA) e *Cooperative Cyber Defense Center Of Excellence* (CCDCOE) (HEALEY & JORDAN, 2014, p. 2). A CDMA tem como missão, sob o comando do *Cyber Defense Management Board* (CDMB), iniciar e coordenar as medidas de ciberdefesa, rever as capacidades e conduzir uma apropriada gestão de riscos dentro da aliança (PERNIK, 2014, pp. 4-5). Além disto também auxilia os estados-membros a melhorar as suas próprias capacidades de ciberdefesa (HEALEY & JORDAN, 2014, p. 2). Contudo, em 2011, deixou de existir o CDMA e passou apenas a existir a CMDB, que é constituído por pessoal especializado ao nível político, militar, operacional e técnico. Além do que foi anteriormente mencionado quanto ao seu propósito, serve também como uma entidade facilitadora para a implementação de políticas de ciberdefesa da OTAN e de capacidades (PERNIK, 2014, p. 5). Tem, igualmente, como responsabilidade, a coordenação da ciberdefesa através dos organismos civis e militares da OTAN. Já o CCDCOE não desempenha uma missão de carácter operacional, mas sim uma função de suporte à Aliança e aos estados-membros, através do melhoramento da interoperabilidade e de capacidades, do desenvolvimento de doutrina, de formação e treino (HEALEY & JORDAN, 2014, p. 2). Paralelamente,

no âmbito da reforma das agências da OTAN, em 2012 foi criada a NATO *Communications and Information Agency* (NCIA), sendo esta entidade responsável por implementar e operar as capacidades de ciberdefesa da Aliança juntamente com as autoridades militares da mesma (NATO *Military Authorities* - NMA) (PERNIK, 2014, p. 5).

No entanto, para fazer face aos pedidos de desenvolvimento de uma capacidade para auxiliar os aliados, que procuram o apoio da OTAN em questões de proteção ou de resposta a ameaças, criaram-se duas equipas de reação imediata (*Rapid Reaction Teams* - RRTs). Estas equipas apenas providenciam assistência técnica limitada, isto é, auxiliam na proteção e na reparação dos sistemas ou coordenam a resposta aos ciberincidentes. Contudo, o seu principal valor é político pois é através destas equipas que se demonstra o comprometimento da Aliança relativamente ao apoio prestado aos seus próprios sistemas e aos aliados que sofram um ataque (HEALEY & JORDAN, 2014, p. 2). Sendo assim, qualquer estado pertencente à Aliança, que esteja sob um ciberataque, pode requerer assistência às RRTs através do CDMB tendo que tal ser previamente autorizado pelo NAC (PERNIK, 2014, p. 5).

É igualmente essencial mencionar a Cimeira de Lisboa, em 2010, na qual se definiu um novo conceito estratégico da OTAN, o qual menciona que esta irá assegurar que dispõe "*the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. (...)*". Uma das medidas a adotar era o desenvolvimento da capacidade da OTAN:

> "*(...) to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations;*" (Heads of State and Government, [s.d], p. 5)

No mesmo ano surgiu uma entidade designada por *Emergency Security Challenges Division* que analisa, entre outras ameaças assimétricas, as ciberameaças (PERNIK, 2014, p. 5). Contudo, os líderes da NATO reconheceram que este domínio "cyber" (Ciberespaço) irá ser cada vez mais usado em eventuais conflitos futuros pelo que, também na Cimeira em Lisboa, se considerou a integração da ciberdefesa no Processo de Planeamento de Defesa da OTAN (NATO's *Defense Planning Process* -

NDPP) iniciado em 2012. De igual modo, os chefes de Estado comprometeram-se a rever a Política de Ciberdefesa da NATO (HEALEY & JORDAN, 2014, p. 2).

Passaremos, agora, a descrever como a OTAN se encontra nos dias de hoje relativamente a esta matéria. As ações mais importantes tomadas pela OTAN foram a criação da Política de Ciberdefesa (NATO *Cyber Defense Policy*), anteriormente mencionada, e o Plano de Ação de junho de 2011 (*Action Plan of June* 2011). Estas ações têm o intuito de fortalecer as bases doutrinárias e de planeamento para a edificação das capacidades cibernéticas, assim como as respetivas estruturas de governança. Estes documentos visam melhorar a capacidade de resposta da OTAN e também ampliar a formação (treino) e providenciar assistência, de modo a prosperar as defesas aliadas bem como as suas capacidades (HEALEY & JORDAN, 2014, pp. 2-3).

Para implementar as medidas/políticas e capacidades definidas nestes documentos o CDMB criou um acordo designado por "*Memoranda of Understanding*" que foi assinado pela autoridade competente de cada estado-membro. Segundo este acordo, cada progresso desenvolvido por parte de um Estado deve ser reportado à entidade máxima responsável pela Aliança, o NAC. Além disto, também existe um novo e permanente Comité de Ciberdefesa (*Cyber Defense Committee* - CDC) que é responsável por gerir a política de ciberdefesa de uma forma genérica, bem como em termos governamentais, incluindo igualmente as capacidades cibernéticas. Por outras palavras, este comité aconselha e supervisiona os países aliados relativamente aos esforços desempenhados na ciberdefesa da NATO (HEALEY & JORDAN, 2014, p. 3). Assim, sempre que um incidente que ocorra tenha implicações políticas, os esforços desempenhados ao nível da ciberdefesa da NATO começam por ser tratados no NCIRC passando seguidamente para o CDMB e finalmente para o CDC, após a respetiva autorização proferida pelo NAC. Além destas principais entidades, existem ainda outras (além das referidas anteriormente) que contribuem para uma melhor eficácia das capacidades de ciberdefesa, como o Comando NATO *Allied Command Transformation* (ACT) e o NATO C3 BOARD (NC3). O primeiro é responsável pelo planeamento e condução do exercício anual (Cyber Coalition Exercise) e pela coordenação do trabalho desenvolvido pelo CCDCOE. O segundo constitui o comité principal para consulta, comando e controlo de aspetos técnicos relativos à ciberdefesa (HEALEY & JORDAN, 2014, pp. 3-4).

Também em 2013, a OTAN criou e acrescentou um conjunto de políticas e medidas operacionais para melhorar as capacidades da Aliança para fazer face aos ciberataques, passando a ser um assunto prioritário entre as prioridades da organização. Ao nível político, na primeira reunião ministerial de defesa da OTAN unicamente dedicada à ciberdefesa, os ministros concordaram em fortalecer as capacidades de ciberdefesa da organização através da expansão da proteção das próprias redes e todas as que são operadas pela aliança e incluindo, também, a ciberdefesa mencionada no processo de planeamento de defesa da OTAN (NDPP). A nível operacional, o processo "Smart Defense", no âmbito da ciberdefesa, foi abordado através do desenvolvimento de três projetos. Um deles, designado *por Multinational Cyber Defense Capability Development* (MNCD2), tem como propósito melhorar os meios para a partilha de informação técnica assim como promover o conhecimento situacional de ameaças e ataques e ainda detetar atividade maliciosa. Um outro projeto foi a criação da *Malware Information Sharing Plataform* (MISP) (NATO, 2013) que é responsável pelo desenvolvimento de uma capacidade da OTAN, acessível a todos os membros, através da qual os estados-membros se comprometem a partilhar informação sobre as características técnicas do malware sem, necessariamente, partilhar os detalhes do ataque (HEALEY & JORDAN, 2014, pp. 4-5). O terceiro e último projeto é designado por *Transatlantic Defence Technological and Industrial Cooperation*, o qual refere as parcerias com a indústria (PERNIK, 2014, p. 7). Também é essencial referir um projeto, igualmente importante, designado por *Multinational Cyber Defence Education and Traning Project* (MNCD E&T), que é liderado por Portugal. Este projeto tem como finalidade o desenvolvimento de uma Plataforma de Coordenação da Educação e Treino em ciberdefesa para proporcionar iniciativas de modo a colmatar as lacunas na educação e treino em ciberdefesa tanto ao nível da OTAN como nos restantes estados. Este projeto é vital pois tanto a educação como o treino contribuem para o desenvolvimento de competências interligadas com as capacidades de ciberdefesa (Governo de Portugal, [s.d]).

Em 2014, na cimeira do País de Gales, foi anunciado uma nova Política de ciberdefesa na Aliança Atlântica bem como o seu plano de implementação. Com esta recente política pretende-se introduzir uma nova postura quanto à colaboração com a indústria através da NATO *Industry Cyber Partnership* (NICP) e reforçar o quadro para o desenvolvimento de capacidades dos aliados e dar enfâse na formação assim como na

educação. A OTAN reconhece a dificuldade de manter um adversário afastado dos sistemas pelo que a resiliência dos seus próprios sistemas bem como das suas defesas é fundamental para assegurar a sua segurança de modo a cumprir os objetivos estratégicos. Esta política mostra que a ciberdefesa está interligada com a defesa coletiva e que também a legislação internacional é aplicável ao ciberespaço. Estes pontos foram incluídos pela primeira vez num documento referente à ciberdefesa uma vez que a aplicabilidade da defesa coletiva ao ciberespaço é uma medida importante de reafirmação e de dissuasão (HEALEY & JORDAN, 2014, p. 5).

3.2 União Europeia – UE

A União Europeia, sendo uma organização político-económica, e quando comparado com a OTAN, considera relevantes outras áreas relativas ao ciberespaço. De facto, as principais áreas de responsabilidade da UE respeitantes à cibersegurança, abrangem questões de segurança interna (tais como: a cooperação na justiça criminal e policial no combate ao cibercrime e a proteção das infraestruturas críticas) e de cooperação internacional. Comparativamente com a OTAN, a UE demorou mais tempo a identificar os aspetos que a cibersegurança apresenta no âmbito da defesa e da segurança nacional. Apenas em 2008, identificou as ciberameaças, que juntamente com a sua dimensão política e económica, também podiam deter um carácter de dimensão militar. Até então, a UE somente lidava com a segurança das redes e da informação, com o cibercrime e, de uma forma menos evidente, com o ciberterrorismo (PERNIK, 2014, p. 2).

Assim, esta temática atraiu a atenção da UE devido às crescentes atividades ilícitas perpetradas no ciberespaço nos finais dos anos 90, pelo que a Comissão Europeia (CE) procurou incitar os Estados-membros a alterarem a forma de atuação perante o cibercrime[3]. Posto isto, em 2001, na Convenção de Budapeste, fora dado ênfase a esta temática pelo que a CE instigou os Estados-membros a combaterem esta nova ameaça (FERNANDES, 2014, pp. 2-3). Conforme indicado na convenção "*Convention on cybercrime*", em Budapeste, é necessário existir uma cooperação entre os estados assim como com a indústria para fazer face ao cibercrime. Para além disto,

[3] Cybercrime – "The use of cyberspace for criminal purposes as defined by national or international law" (GODWIN III, KULPIN, RAUSCHER, & YASCHENKO, 2014, p. 29)

torna-se, também, essencial adotar uma política criminal comum a todos os estados membros através de um enquadramento legal apropriado (COUNCIL OF EUROPE, 2001, p. 1). Durante os dois anos seguintes, de entre os vários documentos produzidos, ficaram estabelecidas as bases para a criação da Agência Europeia para a Segurança das Redes e da Informação ("*European Network and Information Security Agency*" - ENISA) (FERNANDES, 2014, pp. 3-4). Assim, em 2004, a ENISA foi criada com o intuito de garantir um elevado e eficaz nível de segurança das redes e da informação assim como desenvolver uma cultura de segurança das redes e da informação em prol das empresas e organizações do setor público da UE. A ENISA tem como objetivos, de uma forma genérica, a investigação/pesquisa, o desenvolvimento e a assessoria em matéria de segurança das redes e da informação, isto é, reforça a capacidade dos Estados-membros relativa à matéria de prevenção, tratamento e resposta a problemas na segurança das redes e da informação, prestar assistência, aconselhamento e apoio aos Estados-membros e à Comissão e também desenvolver um alto nível de capacidade especializada (Regulamento (CE) 460/2004, p. 4). Contudo, a ENISA sofreu uma transformação devido a fatores de índole diversa como seja o aumento da relevância dos assuntos relacionados "com a dimensão política de segurança do ciberespaço" (FERNANDES, 2014, p. 40) e com a política internacional, bem como o aumento de intrusões, roubo de propriedade e outros incidentes que as demais organizações foram sujeitas, isto é, as consequências do cibercrime entre outras atividades ilícitas. Portanto, a ENISA "opera, de forma indireta, em todos os EMs por iniciativa própria, normalmente em parceria com aqueles ou quando solicitada pelos mesmos" (EM – Estados-membro) (FERNANDES, 2014, p. 41). Sendo assim, a ENISA disponibiliza conhecimento, aconselha e avalia as práticas cibernéticas efetuadas pelas instituições da UE e pelos Estados-membros. Além disto, também facilita o diálogo entre os vários intervenientes da UE na temática da cibersegurança e é a entidade que concebe os exercícios cibernéticos (PERNIK, 2014, p. 18). O mandato da ENISA foi prolongado por um período de sete anos, a contar a partir de 2013, pelo Parlamento Europeu (PE) e pela CE (FERNANDES, 2014, p. 39).

Entretanto, devido à crise económica de 2008, diversas vulnerabilidades estruturais da economia europeia foram expostas. Sendo assim, o principal objetivo da Europa era assegurar um futuro sustentável a curto prazo pelo que a CE, no ano de 2010, criou a estratégia "Europa 2020". Esta estratégia define as linhas de ação para que

a Europa recupere da crise e prepare a economia da UE para o futuro. É constituída por sete iniciativas sendo a Agenda Digital (*Digital Agenda*) elaborada pela CE (DG Connect – Directorate General for Communications Networks, Content and Technology), umas delas. A Agenda Digital pretende definir a importância do papel que a utilização dos sistemas TIC desempenhará na Europa. A Agenda Digital é constituída por sete pilares, dos quais, no Pilar III (*Cibercriminalidade crescente e o risco de confiança nas redes*/*Trust & Security*) está um conjunto de ações essenciais para que os utilizadores do ciberespaço se sintam seguros e protegidos de eventuais atividades ilegais como é o caso da cibercriminalidade. Devido à eficácia de um plano de ação, a UE, para proteger as infraestruturas de informação críticas, desenvolveu várias medidas respeitantes à segurança das redes e da informação assim como ao combate ao cibercrime. Como exemplo, temos a criação de uma "rede ampla e funcional de equipas de resposta a emergências informáticas" (COM(2010)245, 2010, p. 20) (*Computer Emergency Response Team* - CERT) para instituições europeias, agências e organismos, designada por CERT-EU. Este funciona como ponto de contato para auxiliar na prevenção do cibercrime e atuar no caso de emergências como os ciberataques. De igual modo, este pilar da *Digital Agenda* refere que todos os Estados-membros devem ter uma rede funcional, a nível nacional, de CERT que permita providenciar cobertura em toda a Europa (COM(2010)245, 2010, p. 21).

A UE sempre teve como objetivos promover a democracia, a universalidade dos direitos do Homem, o princípio da igualdade, entre outros. Sendo assim, a União sentiu necessidade de estabelecer parcerias com outros Estados e com organizações internacionais que partilhem dos mesmos objetivos. Tendo por base esses princípios e objetivos, o Conselho Europeu consegue identificar os interesses estratégicos da EU pelo que desenvolveu uma Política Externa e de Segurança Comum (*Common Foreign and Security Policy* - CFSP) sendo executada pelo Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança. O Alto Representante é apoiado pelo Serviço Europeu de Ação Externa (*European External Action Service* - EEAS) no cumprimento da política previamente mencionada, trabalhando em cooperação com os serviços correspondeste dos Estados-Membros. Contudo, a UE desenvolveu, de igual modo, uma Política Comum de Defesa e Segurança (*Common Security and Defence Policy* – CSDP/PCDS) de modo a garantir uma capacidade operacional a União tanto em meios civis como em meios militares, constituindo uma parte integrante da CFSP.

Ou seja, a CSDP permite à UE desempenhar um papel nas operações de manutenção da paz, na prevenção de conflitos e reforçar a segurança internacional. Além disto, permite, também, aos membros da UE reunir os seus recursos e desenvolver capacidades de defesa por forma a poderem atuar eficientemente e rapidamente (UNIÃO EUROPEIA, 2012, pp. 28-41). Tal como aconteceu com a CFSP, a UE criou a Agência Europeia de Defesa (*European Defence Agency* - EDA) de modo a garantir que o que está estipulado na CSDP seja cumprido pelos Estados-membros e fornece indicações para que estes melhorem as suas capacidades de defesa assim como as da UE (Decisão 2011/411/PESC DO CONSELHO). Isto é, a EDA está encarregue de ajudar no desenvolvimento das capacidades cibernéticas da UE (PERNIK, 2014, p. 3).

Devido ao crescente número de ciberataques, a Comissão Europeia advertiu para este aumento significativo deste tipo de ameaça pelo que a UE desenvolveu, em 2010 uma abordagem mais estratégica através da Estratégia de Segurança Interna de 2010 (*Internal Security Strategy: Five steps towards a more secure Europe*) focando-se no cibercrime, nas parcerias com a indústria e no desenvolvimento de capacidades (PERNIK, 2014, p. 2). Nesta estratégia são definidos cinco objetivos, dos quais o terceiro (*Raise levels of security for citizens and business in cyberspace*) é constituído por três ações. Dessas ações, a primeira menciona que a UE deverá estabelecer, em 2013, um centro de combate ao cibercrime visto que esta ameaça está em crescimento e que a Europa é o alvo ideal para que sejam perpetrados ataques desta natureza (COM(2010)673, 2010, p. 9). Assim, em janeiro de 2013 foi estabelecido o Centro Europeu de cibercriminalidade (*European Cyber Crime Center* – EC3) tendo sido integrado no Serviço de Polícia Europeia (*European Police Office* - EUROPOL), sendo também apoiado por agências como a ENISA e a Unidade de Cooperação Judicial (*Judicial Cooperation Unit* – EUROJUST) (FERNANDES, 2014, pp. 51-52). Esta entidade desempenha um papel essencial no combate ao cibercrime através do estabelecimento de cooperação entre os promotores e o CERT-EU (PERNIK, 2014, p. 18). Quanto ao EC3, este funciona como ponto de convergência no combate à cibercriminalidade da UE, isto é, atua uma entidade que junta todas as informações associadas ao cibercrime, reúne conhecimentos para apoiar o reforço das capacidades dos Estados-membros, presta também apoio nas investigações dos membros da UE relativos ao cibercrime e atua como interlocutor coletivo dos investigadores europeus junto das autoridades policiais e do poder judicial. Nas competências do EC3, nos

cibercrimes perpetrados às infraestruturas críticas e sistemas de informação da UE estão incluídos os ciberataques às mesmas (COM(2012)140, 2012, pp. 3-6).

Tal como foi mencionado previamente, os casos de ciberincidentes estão a aumentar a um ritmo elevado, tendo já a economia da UE estado sujeita a atividades de cibercriminalidade perpetradas no setor privado e a individualidades. O aumento da espionagem económica efetuada no ciberespaço formula uma nova ameaça aos estados e às empresas da UE. Do mesmo modo, em países não pertencentes à União, os governos poderão recorrer ao ciberespaço para efetuar ações de vigilância e de controlo sobre os seus próprios cidadãos. Sendo assim, a UE promove a liberdade *online* e assegura o respeito pelos direitos fundamentais quando os seus cidadãos estiverem ligados. Posto isto, a UE decidiu, em 2013, desenvolver a sua própria estratégia (*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*) (EU-ECS). Nesta estratégia são definidos cinco princípios gerais de atuação para a cibersegurança, assim como, cinco prioridades estratégicas e as consequentes ações. Estas prioridades são: atingir a ciber resiliência; reduzir drasticamente o cibercrime; desenvolver uma política de ciberdefesa e capacidades relacionadas com PCSD; desenvolver recursos industriais e tecnológicos para a cibersegurança; e por último estabelecer uma política coerente internacional para o ciberespaço (UE, 2013, pp. 4-5). Neste documento são definidas as políticas e os objetivos para o ciberespaço, servindo, também, de base para que cada instituição saiba o que fazer e conseguir efetuar a respetiva monitorização (FERNANDES, 2014, p. 88). Contudo, entre as várias diretivas, é essencial fazer referência à diretiva NIS (*Network and Information Security Directive*). Esta diretiva foi adopta pelo Parlamento Europeu a 6 de julho de 2016 e afirma que os EM terão 21 meses para transpôr a diretiva para as leis nacionais e mais 6 meses para identificar os operadores dos serviços essenciais (EUROPEAN COMMISSION, 2016). Portanto, a diretiva serve para garantir que exista um elevado grau de Segurança das Redes e da Informação (SRI/NIS). Ou seja, é fundamental que se desenvolva e se estabeleça um sistema cooperativo ao nível da União de modo a permitir a troca de informação bem como uma resposta e deteção coordenada de eventuais ameaças que ponham em causa a SRI. Para que este sistema seja eficaz é necessário que todos os Estados-membros tenham o mínimo requerido de capacidades, assim como uma estratégia que garanta um alto nível da SRI a nível nacional. Posto isto, para garantir que o que foi anteriormente mencionado seja cumprido, esta diretiva

define um conjunto de medidas, tais como: instituir obrigações que os Estados-membros terão que cumprir respeitantes à prevenção, à resposta e à forma de como lidar com os riscos e incidentes que afetam as redes e os sistemas de informação; criar um sistema de cooperação entre os estados e estabelecer os requisitos de segurança para as administrações públicas (COM(2013)48, 2013, pp. 11-18). Assim, esta diretiva declara que cada Estado-membro deverá adotar uma estratégia nacional SRI, na qual estejam definidos os objetivos estratégicos assim como as políticas e as medidas regulamentares por forma a obter um elevado nível de SRI. Estas estratégias nacionais deverão mencionar diversos pontos essenciais para atingir esse fim. De igual forma, esta diretiva afirma que cada membro da União deverá ter uma autoridade nacional competente para a SRI bem como estabelecer uma CERT (COM(2013)48, 2013, pp. 19-20). Isto para que haja a criação de uma rede de CERT/CSIRT (*Computer Security Incident and Response Team*) ao nível da UE (PURSER, 2016). Também, nesta mesma diretiva, estão definidos os pontos essenciais para a realização de um plano de cooperação entre os membros da UE (COM(2013)48, 2013, pp. 21-24).

A Diretiva SRI estabelece novos requisitos para a segurança da informação e das redes relativamente aos operadores de serviços essenciais e aos fornecedores dos serviços digitais (DSP's – *Digital Services Providers*). Em adição, também será necessário que essas organizações relatem determinados incidentes de segurança às autoridades competentes ou às CSIRT's. Entende-se como operador de serviços essenciais uma entidade que providencie um serviço fundamental para a manutenção das atividades económicas ou críticas para a sociedade, desde que esse mesmo serviço dependa das redes e dos sistemas de informação. Apenas as organizações que operam com determinados setores é que se encontram listadas na Diretiva SRI. Estas são operadores de serviços essenciais, como por exemplo, o setor enérgico, o sector de transportes, o setor dos serviços financeiros, os serviços de saúde e de fornecimento de água, assim como os serviços de infraestruturas digitais. Portanto, a Diretiva SRI estabelece um conjunto de normas de qualificação, de acordo com as novas regras de relatos de incidentes e de segurança, nas quais, cada membro da UE, se baseia para determinar quais as organizações que obedecem ou não às obrigações expressas na diretiva e assim podendo ou não serem consideradas operadores de serviços essenciais. Por outro lado, os DSP's providenciam um mercado digital, um motor de busca *online* ou um serviço "cloud". Contudo, os DSP's estão sujeitos a menos obrigações que o

operadores de serviços essenciais. Isto é, a Diretiva SRI não estabelece normas para que os Estados determinem quais os DSP's que se enquadram no novo quadro regulamentar. Os DSP's que operem em mais do que um estado-membro da UE estarão somente sujeitos às regras nacionais SRI transpostas na Diretiva, no entanto, os DSP's que não se encontram estabelecidos na União, mas que oferecem os seus serviços à mesma, estão sujeitos a esta Diretiva SRI, tendo que escolher um representante (OUT-LAW.COM, 2016).

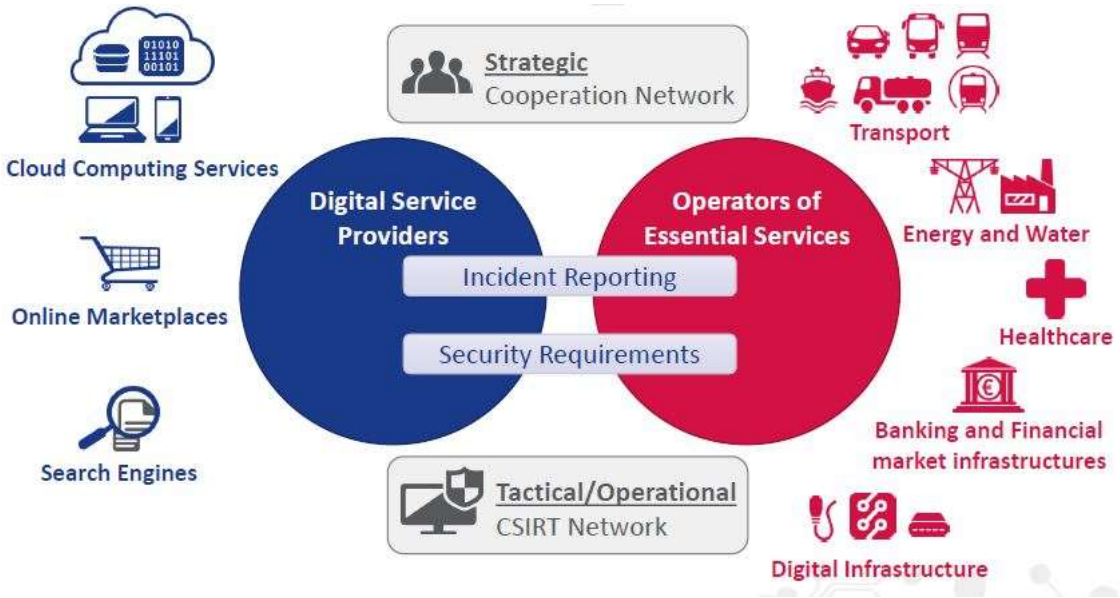

Figura 3 - Diretiva SRI (retirada da apresentação "Implementing The NIS Directive" realizada por Steve Purser a 14ABR16)

Por conseguinte, pode-se verificar que a União Europeia, devido à Diretiva SRI, passará a desempenhar um papel de regulador através do estabelecimento de políticas, expressas na diretiva, relacionadas com a segurança das redes dos estados-membros.

Conforme o que foi previamente mencionado, o terceiro objetivo estratégico estabelecido na EU-ECS (*Developing cyberdefence policy and capabilities related to the framework of the Common Security and Defence Policy* (CSDP)) declara que os esforços da UE também envolvem a ciberdefesa. Isto é, para aumentar a resiliência dos sistemas de comunicações e de informação que apoiam na defesa dos membros e os interesses de segurança nacional, o desenvolvimento da capacidade de ciberdefesa deverá focar-se na deteção, na resposta e na recuperação de ciberameaças. Na EU-ECS estabeleceram-se várias atividades fundamentais, sendo uma delas o desenvolvimento

de uma Política de Ciberdefesa (EU *Cyber Defence Policy Framework*) para proteger as redes de acordo com as missões e as operações da CSDP (UE, 2013, pp. 11-12). Assim, a EDA, com o apoio dos Estados-membros, desenvolveu essa Política de Ciberdefesa em novembro de 2014. Este documento tem como objetivo providenciar um quadro estrutural para os aspetos de ciberdefesa referidos na EU-ECS. Também identifica as áreas prioritárias para a CSDP relativas à ciberdefesa e esclarece o papel a desempenhar por cada um dos intervenientes da UE (UE, 2014, pp. 2-3).

3.3 Comparação entre OTAN e UE

Pode-se constatar que ambas as organizações consideram a cibersegurança um assunto estratégico que influencia a defesa e segurança dos Estados-membros assim como as próprias organizações. Tanto a OTAN como a UE priorizam a resiliência e defesa das suas próprias redes, organizações e missões deixando a cibersegurança, de cada membro, como uma responsabilidade nacional, isto é, cada Estado-membro é responsável pela segurança do seu ciberespaço de interesse. Relativamente a esta temática, as missões de ambas as organizações são complementares, isto é, a OTAN foca-se nos aspetos de segurança e de defesa da cibersegurança enquanto a UE lida de uma forma mais genérica abrangendo a componente não militar deste domínio bem como com os aspetos internos de segurança. Assim, ambas as organizações reconheceram a cibersegurança como uma prioridade estratégia. Existem interesses e atividades não militares comuns entre as organizações. Contudo, a OTAN não dispõem de um mandato para exercer autoridade ou para providenciar orientações relativas às infraestruturas civis do setor privado, o mesmo já não acontece com a UE. Também é fundamental mencionar que as duas organizações diferem na assistência providenciada aos Estados-membros, ou seja, os aliados podem pedir assistência à OTAN através das RRTs enquanto que os membros da UE não conseguem pedir auxílio pois esta não está apta para fornecer a devida assistência técnica ou providenciar os seus serviços (PERNIK, 2014, p. 8). Conclui-se, então, que a OTAN prende-se mais com a questão militar dos seus membros enquanto que a UE prende-se mais com as políticas (*policy*).

Assim, de acordo com o que está disposto anteriormente, conclui-se que a questão derivada QD2: *"O que é que a OTAN e a UE dispõem em termos de*

organização, doutrina, políticas e entidades no âmbito do ciberespaço?" se encontra respondida.

4. Em Portugal e nos Ramos das Forças Armadas

No anterior capítulo efetuou-se um estudo para compreender o que é que a OTAN e a UE dispõem em termos de organização, de estrutura, de doutrina e de políticas, identificando-se as diferenças entre elas no que respeita este quinto domínio. Neste contexto, neste capítulo iremos mencionar de uma forma genérica o que é que o nosso país realizou ao nível do ciberespaço e o que existe relativamente à organização, à doutrina e políticas, incluindo, também, o que os diferentes ramos das Forças Armadas dispõem. Seguidamente, iremos focar-nos mais ao pormenor na Marinha, a fim de aferir como está organizada e que é que dispõem relativamente a esta matéria.

4.1 A nível Nacional

Uma vez que os custos na área das TIC na Administração Pública (AP) sofreram alterações, houve a necessidade de se implementar uma estratégia global para a racionalização das infraestruturas TIC AP. Para que tal acontecesse, foi constituído o Grupo de Projeto para as Tecnologias de Informação e Comunicação (GPTIC), com mandato até 31 de Dezembro de 2015. Este grupo teve como objetivo desenvolver uma estratégia global para a racionalização as TIC na Administração Pública por forma a melhorar a eficiência e a diminuição dos custos associados (RCM 46/2011, 14 de novembro). Por conseguinte, o GPTIC desenvolveu um plano de ação de modo a cumprir com aqueles objetivos. Este é composto por vinte e cinco medidas de racionalização tendo por base cinco eixos de atuação, dos quais apenas o primeiro, designado "Melhoria dos mecanismos de governabilidade", é o que nos interessa para o desenvolvimento deste trabalho. Neste primeiro eixo de atuação são propostas cinco medidas, das quais, a quarta medida consiste na "definição e implementação de uma estratégia nacional de segurança de informação" (RCM 12/2012, 7 de fevereiro). A Estratégia Nacional de Segurança de Informação (ENSI) define os objetivos nacionais para a segurança de informação, a responsabilidade na segurança de informação, a

organização e os serviços da mesma e também a sua gestão. Sendo assim, a ENSI compreende a "criação, instalação e operacionalização de um Centro Nacional de Cibersegurança" (CNCseg/CNCS) (RCM 12/2012, 7 de fevereiro) pelo que o desenvolvimento desta quarta medida foi coordenada pelo Gabinete Nacional de Segurança (GNS) juntamente com a colaboração de entidades essenciais respeitantes a esta matéria (RCM 12/2012, 7 de fevereiro).

Em 2012 foi criada a Comissão Instaladora do CNCseg que tinha como finalidade definir as medidas e os instrumentos essenciais para a constituição do CNCseg (RCM 42/2012, 13 de abril). Desta forma, o CNCseg foi criado na dependência do GNS, alterando a orgânica deste serviço através do Decreto-Lei nº 69/2014 de 9 de maio. Ou seja, recorreu-se a uma adaptação da organização e funcionamento do GNS às funções exigidas pela cibersegurança. O CNCseg tem como missão garantir que o país use o ciberespaço de "forma livre, confiável e segura" (DL 69/2014, 9 de maio), através da cooperação internacional e da "implementação de medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações" (DL 69/2014, 9 de maio), como ciberincidentes ou ciberataques, que, eventualmente, possam pôr em causa o funcionamento das infraestruturas críticas e os interesses nacionais (DL 69/2014, 9 de maio).

Tal como os outros países da UE, Portugal desenvolveu uma estratégia para garantir a segurança e a proteção dos interesses nacionais no ciberespaço. Esta estratégia surgiu em 2015 designando-se por "Estratégia Nacional de Segurança do Ciberespaço"(ENSC). Este documento estabelece as linhas de ação assim como os objetivos de modo a haver uma eficaz gestão de crises, uma coordenação de resposta a ciberataques, um desenvolvimento de sinergias nacionais e também um aumento da cooperação nacional, europeia e internacional no ciberespaço. De igual forma, esta estratégia compromete-se a aprofundar a segurança das redes e da informação por forma a garantir a proteção e segurança das infraestruturas críticas e dos serviços essenciais de informação (RCM 36/2015, 12 de junho).

A ENSC assenta-se em cinco pilares (subsidiariedade; complementaridade; cooperação; proporcionalidade e sensibilização) e desenvolve-se em torno de quatro objetivos, a saber (RCM 36/2015, 12 de junho[4]):

- Promover uma utilização consciente, livre, segura e eficiente do ciberespaço;
- Proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos;
- Fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços essenciais nacionais;
- Afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação.

As implicações e as necessidades associadas a esses objetivos permitem definir uma orientação geral, consubstanciada em seis eixos de intervenção (RCM 36/2015, 12 de junho). O primeiro eixo "Estrutura de Segurança do Ciberespaço" é o de maior relevância para o objetivo deste capítulo. Neste eixo, são estabelecidas medidas para simplificar os desafios que a segurança do ciberespaço exige. Uma dessas medidas refere a necessidade de consolidar o papel do CNCseg como coordenador operacional e de autoridade nacional em matéria de cibersegurança. Uma outra medida, presente neste mesmo eixo, é o desenvolvimento da capacidade de ciberdefesa (RCM 36/2015, 12 de junho).

Como vimos no capítulo anterior, na EU-ECS, uma das prioridades estratégicas definidas é o desenvolvimento da política e das capacidades de ciberdefesa dentro do quadro da CSDP pelo que em 2013 foi publicado a Orientação Política para a Ciberdefesa. Esta Orientação Política tem como finalidade determinar os princípios fundamentais, definir os objetivos e estabelecer as consequentes linhas de ação, de modo a desenvolver uma capacidade nacional de ciberdefesa. Esta política de ciberdefesa define três objetivos: garantir a resiliência, a proteção e a segurança das redes e das TIC contra ciberataques; assegurar a liberdade de ação no ciberespaço e, quando necessário, atuar por forma a impedir ou dificultar um ato hostil contra os interesses nacionais; contribuir de modo cooperativo para a cibersegurança nacional. Para se cumprir com os objetivos estabelecidos foram definidas linhas de ação, das

[4] A Estratégia Nacional de Segurança do Ciberespaço assim como os objetivos mencionados, encontram-se vertidos nesta RCM.

quais, uma é estabelecer uma estrutura de comando e controlo da ciberdefesa nacional. Assim, Portugal responde a este desafio através da existência de um organismo que tenha um carácter de orientação estratégico-militar quanto às atividades de ciberdefesa e que tenha uma capacidade de resposta a ciberincidentes e a ciberataques (Despacho nº 13692/2013, 28 de outubro do MDN).

Relativamente à matéria de ciberdefesa, a Direção de Comunicações e Sistemas de Informação (DIRCSI) do Estado-Maior General das Forças Armadas tem como missão "coordenar a proteção dos valores de integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas" (DR 13/2015, 31 de julho). De igual forma, coordena a proteção dos mesmos valores, previamente mencionados, mas no âmbito da cibersegurança sectorial da defesa nacional. Portanto, na estrutura da DIRCSI está presente o Centro de Ciberdefesa (CCD) (DR 13/2015, 31 de julho) que, na dependência do CEMGFA, é o órgão responsável pela condução de operações no ciberespaço, assim como pela resposta a ciberincidentes e a ciberataques, tendo responsabilidades de coordenação, operacionais e técnicas (Despacho nº 13692/2013, 28 de outubro). Assim, ao CCD compete a direção e a coordenação da capacidade de ciberdefesa nacional (ex.: condução de operações militares no ciberespaço; promoção de projetos de investigação e desenvolvimento; entre outros); o planeamento, a coordenação e a direção das investigações de ciberincidentes relevantes para a ciberdefesa (ex.: assegurar uma capacidade permanente de deteção, de resposta e de recuperação de ciberincidentes); a coordenação e a cooperação com os Núcleos *Computer Incident Response Capability* (CIRC) dos ramos das Forças Armadas (FA) e do EMGFA; a partilha de informação de modo a colaborar numa resposta defensiva com o CNCseg e com os CIRC nacionais e internacionais; entre outras competências. No âmbito da cibersegurança sectorial, o CCD coopera com as estruturais nacionais responsáveis pela cibersegurança, pela ciberespionagem, pelo cibercrime e pelo ciberterrorismo. Supletivamente, de acordo com as competências associadas à cooperação nacional e internacional do CNCseg, o CCD partilha informação com o CIRC nacionais e internacionais. O CCD é a autoridade técnica da ciberdefesa e da cibersegurança sectorial da defesa nacional (DR 13/2015, 31 de julho).

Ainda relativamente ao primeiro eixo da estratégia nacional, existe uma outra medida fundamental. Esta medida corresponde ao desenvolvimento da capacidade

nacional de resposta a incidentes, ou seja, declara que o papel desempenhado pelas *Computer Incident Response Team* (CSIRT) terá que ser reforçado de modo a funcionar como uma plataforma para a partilha de informação e de boas práticas associadas aos ciberincidentes assim como para os "serviços operacionais de resposta a incidentes" (RCM 36/2015, 12 de junho) nacionais e estrangeiros caso, estes tipos de incidentes, constituam uma ameaça à soberania nacional (RCM 36/2015, 12 de junho).

Importa, agora, descrever o que cada um dos ramos das FA dispõe relativamente a esta matéria e que deverá funcionar desejavelmente em sintonia e alinhamento com o CCD. Iremos falar, de uma forma genérica, sobre o Exército e a Força Aérea e mais detalhadamente sobre a Marinha.

4.2 Exército

Dispõe de duas estruturas, sendo estas, o Sistema de Informação e de Comunicações Operacional (SIC-O) (cobertura nacional) e o Sistema de Informação e Comunicações Tático (SIC-T). Este permite estabelecer o Comando e Controlo (C2) de todas as Unidades/Estabelecimentos/Órgãos (U/E/O) bem como de todas as unidades táticas. O Exército, assim como os restantes ramos, dispõe de um CIRC que tem como finalidade providenciar apoio nas operações ofensivas perpetradas no ciberespaço (CNO), isto é, pode efetuar intrusões de modo a afetar os princípios de segurança (confidencialidade, integridade e disponibilidade) nos sistemas de informação e de comunicações inimigos. O núcleo CIRC do Exército encontra-se no Regimento de Transmissões (RTm); contudo, em contexto operacional, rege-se sob o Comando do Batalhão de Transmissões da Escola Prática de Transmissões (EPT) (PINTO, 2013, pp. 19-20).

4.3 Força Aérea

Neste ramo existe a Direção de Comunicações e Sistemas de Informação (DCSI) que corresponde à parte técnica, ou seja, é responsável pela implementação de políticas e doutrina, pela operação, pela administração e pela sustentação. Da DCSI provêm três repartições: a Repartição de Tecnologias de Informação (RTI); a Repartição de

Segurança da Informação (RSI) e a Repartição de Comunicações e Sensores de Navegação (RCSN). A RSI e a RCSN estão relacionadas com aplicações, análise, programação bem como com as redes, respetivamente. No entanto, na RTI, relacionada com os servidores, está disposta a Secção de Ciberdefesa, desempenhando, neste contexto, as funções de CIRC da Força Aérea. Esta secção tem como funções a monitorização, a auditoria, a reação a incidentes e a sensibilização (palestras e boletins) (Jorge Valente, 2016).

4.4 Marinha

Na Marinha, com o aumento do número de Sistemas de Informação e Comunicações Automatizados (SICA), tornou-se necessário garantir a proteção da informação e dos recursos que auxiliam esses mesmos sistemas. Os SICA garantem o armazenamento, o processamento e a transmissão de informação, de carácter operacional e administrativo, essencial para o cumprimento das missões atribuídas à Marinha pelo que é fundamental a sua proteção (MDN, 2005, p. 1.3). Assim, surge o conceito de SICA da Marinha (SICAM) que é um agregado de "Sistema de Informação e Comunicação, constituído por um SICA ou conjunto de SICA, que apoia de forma directa ou indirecta, o cumprimento da missão de uma das áreas funcionais da Marinha ou de todas estas" (MDN, 2005, p. 1.3). Por conseguinte, por forma a garantir a proteção dos SICA é necessário implementar políticas de segurança, assim como uma estrutura que possibilite a monitorização, a identificação, o alerta, a resposta e a recuperação caso um SICA tenha sido alvo de um comprometimento à confidencialidade, à integridade, à disponibilidade e à autenticação da informação. Neste quadro, tornou-se imperativo implementar na Marinha uma Capacidade de Resposta a Incidentes de Segurança da Informação (CRISI). Esta permite efetuar uma resposta aos incidentes de segurança que estejam relacionados com atividades maliciosas, *software* malicioso, negação de serviços assim como outras ameaças associadas aos SICA, ou seja, responde aos diversos incidentes de segurança da informação na Marinha de forma coordenada (MDN, 2012, p. 1.1).

O desenvolvimento da CRISI resultou da necessidade de cumprir com o que fora estabelecido tanto nas diretivas políticas da OTAN como nas da UE, estando,

igualmente, em alinhamento com o preconizado ao nível do EMGFA (MDN, 2012, pp. 2.1-2.2). Algumas dessas diretivas já foram mencionadas previamente neste trabalho, designadamente: a Declaração de Praga de 21 de novembro (2002); o Conceito Estratégico de Defesa e Segurança da OTAN (2010); o documento que surgiu na Cimeira da OTAN em Lisboa (2010); a Diretiva de Planeamento da Marinha (2014)[5] e por último, a Estratégia Interna da União Europeia.

A CRISI é constituída por um conjunto de pessoas, processos e tecnologia que permite responder e tratar qualquer incidente de segurança que ocorra ao nível dos SICA da Marinha, tendo para isso que se socorrer de meios de análise, de disseminação e de relato da informação associada ao incidente. Além disto, tal como acontece a nível internacional (CSIRT – *Computer Security Incident Response Team*), a CRISI deve adotar uma postura pró-ativa (análise das vulnerabilidades; investigação dos incidentes de segurança; formação; entre outros) de modo a minimizar os riscos de segurança dos SICA (MDN, 2012, pp. 2.2-2.3). Desta forma, a CRISI tem como principal objetivo a prevenção e a diminuição do risco de ocorrência de um incidente de segurança da informação, assim como a minimização do seu impacto nos SICA. No entanto, a CRISI tem outros objetivos, como por exemplo, a gestão eficaz da resposta aos incidentes, a recuperação imediata dos mesmos, entre outros. Sendo assim, disponibiliza três serviços: serviços reativos (ex.: gestão de incidentes; análise de incidentes); serviços pró-ativos (ex.: análise e gestão das vulnerabilidades; serviços de monitorização e deteção de intrusão) e por último os serviços de gestão de segurança e qualidade de serviço (ex.: colaboração na análise de risco; contribuição para a definição dos requisitos). Além destes serviços, a CRISI dispõe, também, de sistemas de apoio como: o Sistema de Registo de Incidentes (efetuar o registo de incidentes e das ações tomadas); o Portal da CRISI (plataforma de apoio à estrutura da CRISI e divulga informação) e Sistemas, equipamentos e tecnologias, que são essenciais para o Grupo de Resposta a Incidentes de Segurança de Informação – GRISI (MDN, 2012, pp. 2.3-2.5).

[5] Anteriormente designada por Diretiva de Política Naval (2011) e que mencionava as mesmas medidas – "criação e partilha dos recursos informacionais que alimentam ferramentas de gestão estratégica (*Balanced Scoreboard e Enterprise Project Management* - EPM), os sistemas de Comando e Controlo (C2) e de defesa do ciberespaço da Marinha, para garantir a exploração integrada daqueles recursos, a uniformização dos requisitos, a eficiência na gestão da informação, a superioridade de conhecimento, de decisão e de execução, e a optimização do Comando e Controlo." (CEMA S. L., 2011)

Após se ter mencionado qual o propósito e o objetivo principal da CRISI bem como quais os seus serviços e os seus sistemas de apoio, passaremos a mostrar como esta se encontra estruturada.

A estrutura da CRISI baseia-se nos recursos humanos, nas entidades de segurança dos SICA assim como noutras estruturas da Marinha. Assim, esta estrutura é composta por três níveis de atuação e coordenação, sendo estes (MDN, 2012, pp. 2.5-2.6):

- Nível 1 – Entidade de coordenação da CRISI (EC-CRISI);
- Nível 2 – Grupo de Resposta a Incidentes de Segurança de Informação (GRISI);
- Nível 3 – Entidades da Organização de Segurança dos SICA.

No primeiro nível encontra-se o Estado-Maior da Armada (EMA) que atua como a entidade de coordenação de resposta a incidentes de segurança de informação, de assessoria jurídica e também estabelece ligações com entidades externas, para além de produzir e manter atualizada a doutrina atinente. Do segundo nível fazem parte as Áreas das Tecnologias de Informação e Operacional, que providenciam apoio na análise, na deteção, na resposta e na recuperação de incidentes de segurança. Da mesma forma, fornecem apoio às Autoridades Operacionais dos SICA (AOSICA)[6] relativo à deteção de intrusão bem como na prevenção de *software* malicioso. Finalmente, as entidades da organização de segurança dos SICA são responsáveis por assegurarem as necessárias condições de segurança e relatar qualquer atividade suspeita associada às suas áreas de competência (MDN, 2012, p. 2.6). A seguinte figura mostra a estrutura e organização da CRISI:

[6] AOSICA – "entidade que garante a operacionalidade do respetivo SICAM, representando, desta forma, toda a comunidade de utilizadores dos SICA que constituem esse SICAM. A sua responsabilidade estende-se, assim a todos os respectivos SICA, desde a fase em que estes são entregues para a operação até ao seu abate." - (MDN, 2005, p. 7.2)

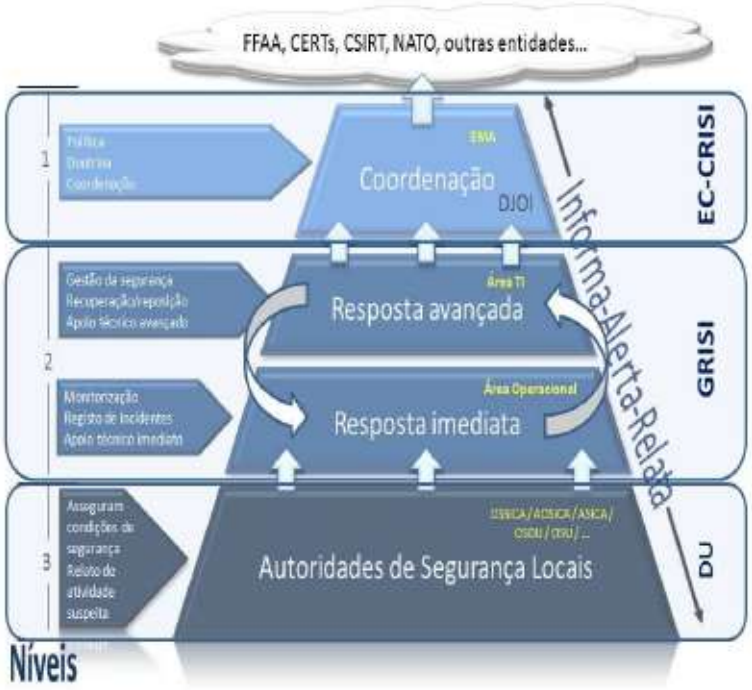

Figura 4 - Estrutura e Organização da CRISI (Retirado do PCA 16)

Conforme apresentado na figura, no segundo nível, o GRISI é constituído por elementos das Áreas das Tecnologias da Informação e Operacional, essenciais no desempenho de tarefas associadas ao ciclo de tratamento de incidentes. Assim, o GRISI é composto por dois subgrupos: Subgrupo de Resposta Avançada e Subgrupo de Resposta Imediata. O primeiro subgrupo é responsável por providenciar apoio técnico caso ocorra algum incidente de segurança da informação assim como é responsável, juntamente com o Subgrupo de Resposta Imediata, pelo ciclo de tratamento dos incidentes (resposta, recuperação, manutenção e prevenção/proteção). O segundo subgrupo é constituído pelo Centro de Comunicações, de Dados e de Cifra da Marinha (CCDCM), sendo este responsável pela ligação direta aos utilizadores no que diz respeito aos incidentes de segurança da informação, ou seja, atua como um centro de recolha, análise e de coordenação de incidentes. Além disto, é igualmente responsável pela deteção e análise de incidentes de segurança (MDN, 2012, pp. 2.7-2.8).

Quanto à gestão de incidentes, esta envolve toda a estrutura e organização da CRISI. Assim, a gestão de incidentes envolve determinadas fases dando origem ao Ciclo de Gestão de Incidentes, como se pode verificar na seguinte figura:

Figura 5 - Ciclo de Gestão de Incidentes (retirada do PCA 16)

Assim, de uma forma sucinta, nas fases de proteção e de prevenção, as infraestruturas, sistemas e serviços assim como a informação armazenada, transferida e processada pelos SICA são monitorizadas, sendo os eventos correlacionados, caracterizados e categorizados em eventos de segurança, se for caso disso. Nas fases de deteção e análise os eventos que foram registados e classificados como incidentes de segurança são triados e priorizados de modo a viabilizar uma resposta imediata pelo Grupo de Resposta Imediata (GRI). Na fase de tratamento de incidentes, caso não exista capacidade para efetuar uma resposta imediata, a sua análise e resolução passa para a área de TI, envolvendo o Grupo de Resposta Avançada (GRA). Contudo, se precisar de apoio na coordenação do incidente, que transcenda a capacidade da GRA, a EC-CRISI é ativada uma vez que, nestas situações, poderá ser necessário coordenar as ações com entidades externas, designadamente o CCD e o CNCSeg. Os incidentes de origem externa são registados nos Sistemas de Gestão de Incidentes, que tem como objetivo dar nota de todas as ações tomadas sobre os incidentes, providenciando à CRISI a capacidade de saber quais os que estão em tratamento e como se encontra o seu processo de resolução. Posteriormente, este tipo de incidentes são analisados na triagem efetuada pelo GRI (MDN, 2012, pp. D.1-D.4). Para um melhor perceção das fases macro da gestão de incidentes, segue-se a seguinte figura:

Figura 6 - Fases Macro de Gestão de Incidentes (retirado do PCA 16)

Toda a informação presente no Sistema de Gestão de Incidentes contribui para a edificação do Panorama Situacional do ciberespaço de interesse para a Marinha e assim do CSC, que atua como uma plataforma virtual, e envolve a informação obtida no Sistema de Gestão de Incidentes.

Deste modo, pode-se concluir que a Marinha dispõe de uma capacidade de cibersegurança nas unidades em terra. Contudo, verifica-se que o mesmo não se pode dizer no que diz respeito às UN quando estas se encontram a navegar em cumprimento das respetivas missões ou atracadas em portos fora da jurisdição da Marinha. Portanto, de acordo com o DOTMLPFI, verifica-se que, em termos de doutrina (D), a Marinha tem publicações, como por exemplo o PCA 2 e o PCA 16 (CRISI), que estabelecem instruções ou normas necessárias para garantir a segurança da informação e para edificar uma capacidade de resposta aos incidentes, ainda que a mesma não contemple, pelo menos explicitamente, o que deve ser feito nas UN. Em termos de organização (O), contatou-se que as unidades em terra estão preparadas e organizadas para exercer a capacidade de cibersegurança. Isto é, detêm uma estrutura concebida para providenciar uma resposta aos ciberincidentes que ponham em causa a segurança da informação. Associada à organização está a liderança uma vez que é essencial para o

desenvolvimento de uma estrutura e por conseguinte uma organização. No entanto, e ainda que maioria das UN da Marinha possuam redes a bordo e as fragatas operem em rede quando inseridas em forças navais, não foi possível identificar doutrina, no âmbito das operações navais, que enquadre qual a organização que deve existir a bordo para edificar conhecimento situacional sobre o ciberespaço de interesse para o navio e como se deve o navio organizar para fazer face a incidentes de cibersegurança quando se encontra em plena atividade operacional.

Relativamente ao treino e formação (T), existe oferta no âmbito da segurança de informação (INFOSEC), sendo exemplos o Curso de Aperfeiçoamento INFOSEC – Segurança dos Sistemas de Informação e Comunicação (AK08) e o Estágio de Segurança de Informação (IDI01). Contudo, ainda não existe, na Marinha, nenhum curso específico na área da cibersegurança. O treino e formação está interligado com o pessoal (P) que opera com os sistemas necessários para atingir o objetivo definido, ou seja, é essencial haver pessoal especializado para estar apto a operar com os diversos sistemas bem como a existência, tal como foi mencionado previamente neste trabalho, de uma cultura de segurança. Este desiderato só é atingido através do treino e da formação. No mesmo contexto, para se poder edificar uma capacidade de cibersegurança é fundamental que as entidades associadas a esta matéria, disponham de material (M) suficiente e atualizado para poderem exercer as suas funções. No entanto, as infraestruturas também desempenham um papel fundamental. Na Marinha, tanto o Centro de Operações de Rede (CORE) da DITIC como parte do CCDCM (CIRC) desempenham funções importantes no combate aos incidentes de segurança da informação. Mas mais uma vez, relativamente às UN, não existem evidências sobre a existência de meios materiais para o propósito de contribuir para o incremento da cibersegurança das UN quando em operações, i.e., quando fora do controlo do domínio marinha.pt.

De facto, ao nível das unidades em terra, existe um enquadramento formal relativamente à doutrina, organização, infraestruturas, entre outras, contudo, por outro lado, nas UN, o mesmo não acontece. Uma vez que os navios estão interligados através de redes, estarão sempre sujeitos a incidentes de segurança de informação sendo provável que alguém se consiga infiltrar na rede de um navio. Por esta razão, é fundamental que, a bordo das UN, exista uma organização mais apropriada para reagir ou lidar com as eventuais intrusões que possam surgir ou com outros tipos de

incidentes. Isto porque a organização existente nos navios cumpre o disposto nas publicações como o PCA 16, o PCA 10 ("Conceito de implementação do SICA no domínio do utilizador") e o PCA 2. Nestas publicações estão definidos alguns cargos como: Oficial de Segurança do Domínio do utilizador (OSDU), responsável pelo cumprimento das normas assim como dos procedimentos de segurança (POPs); o Gestor Operacional do Domínio do Utilizador (GODU) deve conhecer os requisitos funcionais a implementar e a manter no seu domínio do utilizador (DU) e dos requisitos de segurança; o Administrador do Domínio do Utilizador (ADU) deve conhecer as capacidades dos serviços básicos e funcionais e da arquitetura dos requisitos de segurança; entre outros (MDN, 2005, p. 7.7). No entanto esta organização não foi concebida para situações operacionais, designadamente as que se vivem nas UN em operações, importando, por isso, adequá-la a este contexto. Do que foi possível apurar nesta investigação, o que o pessoal das UN poderá apenas fazer (no atual enquadramento), caso ocorra alguma intrusão ou qualquer outro incidente, é comunicar esse facto através do "Relato de Incidente", o qual está disponível no portal da CRISI. Após se ter efetuado o relato do incidente, as UN poderão tentar obter informação sobre a identificação do comprometimento. No entanto, é, também, improvável que isso aconteça visto não existirem a bordo meios para tal, bem como pessoal com formação para efetuar esse tipo de operações.

No caso das fragatas e sempre que estas se encontram operações navais, recorre-se ao uso de salas de *chats* (ex: j-chat), pertencentes a uma rede NATO *Secret Wide Area Network* (NSWAN), para comunicar com os restantes navios, sendo esta rede monitorizada pela DITIC.

Enquanto as unidades em terra estão bem estruturadas dispondo de doutrina, de material e de uma organização essenciais para a capacidade de cibersegurança, as UN não dispõem de uma organização a bordo específica para as questões associadas a esta matéria, nem de pessoal formado, nem de procedimentos assim como de meios para monitorizar a rede e reagir aos eventuais incidentes que ocorram.

Face ao que antecede constata-se haver necessidade de elaborar um enquadramento doutrinário bem como uma organização a bordo das UN para que estas consigam fazer frente a esta nova ameaça quando se encontram envolvidas num determinado teatro de operações no âmbito da OTAN e da UE incluindo também missões sem um elevado conteúdo operacional, estendo, assim, o conceito de

“Capacidade” no âmbito do tema do presente trabalho às UN, quando a navegar no cumprimento da respetiva missão. Assim, conforme o disposto anteriormente, verifica-se que a questão derivada QD3: “*O que é que existe na Marinha Portuguesa, tanto a bordo das Unidades navais como nos Comandos em terra, sobre o CSC?*” se encontra respondida.

5. Conclusões e Recomendações

O ciberespaço é um domínio onde circula uma quantidade cada vez maior de informação, sujeita a diversos tipos de ameaças que podem resultar na falta de integridade, de confidencialidade, de autenticidade e de disponibilidade.

O trabalho realizado nesta dissertação teve como objetivo o estudo do conceito de Conhecimento Situacional no Ciberespaço (CSC), incluindo a forma como o mesmo é aplicado a bordo das UN da Marinha numa lógica de abordagem segundo o conceito de capacidade. Neste estudo, após um breve enquadramento do tema, foi apresentado uma definição dos conceitos de ciberespaço, de cibersegurança e de ciberdefesa, que são essenciais para a compreensão do CSC. O ciberespaço é um domínio composto por diversas camadas, onde se incluem a dos Utilizadores, a Lógica, a do Circuito e a Geográfica. A camada dos Utilizadores é onde todos nós temos acesso ao ciberespaço, sendo da nossa responsabilidade a informação que é colocada e partilhada com os outros. A camada Lógica corresponde às aplicações e protocolos que permitem comunicação entre os utilizadores e entre utilizadores e os sistemas de armazenamento e processamento de informação. A camada Circuito refere-se aos componentes físicos da arquitetura de rede que permite a ligação entre sistemas. Finalmente, a camada Geográfica é onde estão localizados os sistemas de comunicações e de armazenamento de informação, em que a aplicação de legislação e de proteção de dados depende da zona de implementação dos sistemas de informação. Isto é, o ciberespaço permite à população novas oportunidades de acesso e troca de informação, uma vez que proporciona serviços essenciais ao bem-estar das pessoas assim como das sociedades. Tal como foi mencionado previamente no trabalho, o “ciberespaço transpõe a vida real para o mundo virtual”. O ciberespaço é considerado o quinto domínio, em conjunto com

os domínios superfície, ar, mar e espaço. Neste âmbito, o ciberespaço, serve, igualmente, para a realização de operações militares, ou seja, para a guerra.

As sociedades e as pessoas estão mais dependentes do ciberespaço. Desta forma, é importante garantir a segurança da informação que circula neste mesmo domínio. Todos os utilizadores que acedem ao ciberespaço devem ter sempre presente quais as medidas e os procedimentos de segurança a aplicar de modo a fomentar uma cultura de segurança. A INFOSEC é importante para uma melhor compreensão dos conceitos de cibersegurança e de ciberdefesa. Deste modo, a garantia da informação incluí a segurança física dos sistemas e da própria informação, enquanto a INFOSEC está relacionada com a aplicação de medidas e procedimentos de segurança por forma a proteger e preservar a informação oriunda dos sistemas de comunicações e de informação. Todas estas medidas e procedimentos contribuem para a manutenção da confidencialidade, da integridade, da disponibilidade e da autenticidade da informação.

Relativamente à cibersegurança e apesar de não haver uma definição universal, a ITU define-a como um conjunto de políticas, ferramentas, ações que, com o apoio das tecnologias, protegem o ciberespaço, a organização assim como os meios existentes na mesma. Nesses meios estão incluídos os sistemas computacionais, a infraestrutura, o pessoal, os sistemas de telecomunicações bem como toda a informação trasmitida/recebida através do ciberespaço. Quanto à ciberdefesa, o conceito está definido como o conjunto de medidas necessárias para a proteção das infraestruturas TIC contra ciberataques, ou seja, compreende todas as medidas necessárias para a defesa do ciberespaço recorrendo a ações de natureza militar. Assim, na ciberdefesa, estão incluídas as CNO.

O propósito de caracterizar os conceitos de ciberespaço, cibersegurança e ciberdefesa é o de melhor compreender em que consiste o CSC. O recurso ao Ciclo de Boyd (Observar, Orientar, Decidir, Agir) é fundamental para a edificação da capacidade de cibersegurança, de ciberdefesa e assim do CSC. Isto porque, numa COI, a partilha de informação e os laços de confiança entre as pessoas que a constituem são essenciais para a obtenção do panorama do ciberespaço de interesse da COI. Por sua vez, as organizações pertencentes a uma mesma COI, necessitam de ser interoperáveis entre si para obterem um cenário mais completo. Assim, de acordo com os conceitos de cibersegurança e de ciberdefesa, verifica-se que, relativamente às duas últimas fases do Ciclo de Boyd (Decidir e Agir), existem diferenças conforme se trate de atividades no

âmbito da cibersegurança ou da ciberdefesa. Portanto, o CSC consiste em obter conhecimento suficiente para permitir às organizações preverem e assim atuarem ou reagirem de forma atempada e coordenada aos diversos eventos que ocorram no respetivo ciberespaço de interesse. O conhecimento pode ser adquirido através da partilha de informação e da interoperabilidade entre os constituintes de uma COI bem como entre várias COIs, pelo que é essencial a existência de laços de confiança. Contudo, subjacente a um eficiente e eficaz CSC, existem processos, tecnologia e pessoas, que poderão constituir uma das maiores vulnerabilidades de uma organização pelo que é importante que seja implementada de forma sustentada uma cultura de segurança na mesma. Portanto, além de ser útil aplicarmos o Ciclo de Boyd no processo de edificação do CSC também é relevante aplicarmos o conceito de "capacidade" de modo a enquadrar as questões associadas ao CSC de forma holística e assim colmatar as eventuais vulnerabilidades nesses componentes (processos, tecnologia e pessoal), permitindo tornar a cultura de segurança numa determinada organização eficaz e eficiente.

Na segunda parte deste estudo, depois de uma breve introdução à OTAN e à UE, investigou-se sobre o que é que ambas as organizações dispõem em termos de organização, doutrina, políticas e entidades que estejam associadas a este novo domínio. Conclui-se que, embora ambas considerem a cibersegurança um assunto que influencia a segurança e defesa dos Estados, diferem na forma como a operacionalizam. Enquanto que a OTAN se foca principalmente nos aspetos de segurança e defesa incluindo a vertente militar, a UE incide primordialmente nos aspetos internos de segurança da informação, focando-se eminentemente nas respetivas políticas e não incluindo a componente militar,. Também se pôde verificar que diferem na assistência providenciada aos estados-membros; a OTAN providencia ajuda técnica através das RRTs e a UE não está apta para providenciar assistência aos EM. Assim, a UE, além de ter desenvolvido uma estratégia para a segurança do ciberespaço (EU-ECS), estabeleceu diretivas que definem objetivos e políticas que os EM deverão cumprir. Serve de exemplo destes objetivos e políticas a criação de equipas especializadas para garantir a segurança da informação, designadas por CERT, que são responsáveis por providenciar os serviços essenciais para as organizações lidarem com os ciberincidentes e sustentarem a recuperação dos componentes dos sistemas, estando, desta forma, associados à cibersegurança. De entre as diretivas, é importante realçar a Diretiva SRI

(NIS). Esta serve para garantir um elevado nível de segurança da informação e das redes e estabelece novos requisitos para a segurança de informação e das redes referentes aos operadores de serviços essenciais e dos fornecedores dos serviços digitais (DSP). Ou seja, esta diretiva desempenha um papel regulador devido ao estabelecimento de políticas associadas à segurança das redes. Por outro lado, a OTAN, dada a sua natureza de organização político-militar, lida com a ciberdefesa pelo que estabeleceu políticas neste contexto, como é o caso da Política de Ciberdefesa, englobando, também, as entidades que gerem essas mesmas políticas e que supervisionam os esforços efetuados pelos países aliados neste campo, nomeadamente, o NAC, o CDMB, a NCIA, entre outras.

Por conseguinte, após se ter verificado o que estas organizações detêm respeitante ao ciberespaço, de acordo com os componentes do conceito de capacidade (DOTMLPFI), efetuou-se um estudo sobre o que é que Portugal e os diferentes ramos das FA e EMGFA têm relativamente a esta matéria. Neste último capítulo incidiu-se, maioritariamente, na Marinha e nas operações navais, tendo sempre em consideração o conceito de capacidade aplicada à edificação do CSC, com particular enfoque nas unidades navais.

Assim, seguindo uma abordagem "capacitária", verificou-se que Portugal tem estruturas próprias para estar apto a edificar uma capacidade de cibersegurança, residindo o respetivo vértice no CNCseg. No que diz respeito à capacidade de ciberdefesa existe a DIRCSI do EMGFA que inclui o CCD na sua estrutura, sendo responsável pela condução de operações no ciberespaço assim como pela resposta a ciberincidentes e a ciberataques numa lógia conjunta. Em termos de doutrina e políticas, de acordo com o estipulado por parte da UE, Portugal elaborou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) e de modo a desenvolver a capacidade de ciberdefesa criou a Orientação Política para a Ciberdefesa. Além destas entidades, existem os CIRC, tanto a nível nacional como internacional, que são efetivamente a primeira linha na ação (completar), desempenhando, concomitantemente, um importante papel na partilha de informação. Tal como já foi mencionado, para que tal ocorra é necessário a construção, de forma sólida, de laços de confiança entre COIs, que neste caso são o CCD e os CIRC, incluindo um forte nível de interoperabilidade entre eles. Uma das medidas estabelecida na ENSC corresponde ao desenvolvimento de uma capacidade nacional de resposta a incidentes onde é relevado o papel dos CSIRTs. Este

deve funcionar por forma a atuar como uma plataforma de partilha de informação e de boas práticas associadas a ciberincidentes, que possam por em causa a soberania nacional.

Após uma breve explicação sobre o que tanto o Exército como a Força Aérea dispõem relativamente a este quinto domínio, pode-se constatar que ambos detêm de um CIRC. No entanto, devido ao facto deste tema ser relativamente recente, as capacidades de cibersegurança e de ciberdefesa ainda não se encontram completamente implementadas. Seguidamente focou-se o estudo sobre o que a Marinha dispõe sobre este domínio. Constatou-se que este ramo dispõe de uma capacidade para responder a incidentes ao nível INFOSEC designada por CRISI, cujo principal foco é a prevenção e a diminuição do risco de ocorrência de um incidente de segurança da informação. Assenta num modelo de três níveis, correspondendo a cada um uma entidade responsável por efetuar o que lhe compete. A entidade referente ao segundo nível é o GRISI. Esta entidade é composta por elementos provenientes das áreas das tecnologias da informação e operacional e é composta por dois subgrupos de resposta sendo um deles de responsabilidade do CCDCM. O CORE da DITIC também desempenha um papel importante na resposta a incidentes de segurança de informação. Todas estas entidades operam em articulação com o CNCseg e com o CCD pelo que também podemos dizer que operam segundo o conceito de CSC. Deste modo, conclui-se que a Marinha possui uma estrutura assim como uma organização bem definida para as fazer face a ciberincidentes nas unidades em terra.

Ainda na ótica da capacidade, relativamente à doutrina, a Marinha possui diversas publicações, nomeadamente o PCA 16, PCA 10 e o PCA 2, que estabelecem normas e procedimentos para os utilizadores. Quanto à formação, do que foi possível apurar, existem dois cursos no âmbito da segurança da informação, pelo que é importante que se crie um curso mais apropriado no âmbito da cibersegurança e da ciberdefesa. De modo a sensibilizar, treinar e formar o pessoal, estes temas deveriam fazer parte da formação de todos, designadamente, na Escola Naval ou na Escola de Tecnologias Navais (ETNA). Por outras palavras, considera-se que a oferta em formação desta natureza deverá ser alargada na Marinha.

Nas UN, para além do que está definido na doutrina, não existe uma estrutura que, num teatro de operações, consiga atuar perante uma ciberameaça. Uma vez que também não existe pessoal formado, procedimentos e meios fundamentais para a

monitorização das redes, é imperativo que se elabore um enquadramento doutrinário que estabeleça uma organização a bordo das UN para reagir perante este novo tipo de ameaças. Por outro lado, a doutrina estabelecida não inclui a edificação da capacidade de CSC. Neste contexto, afigura-se ser necessário o envolvimento do EMA (para a adequação da doutrina vigente à realidade das UN), do CN (enquanto entidade que promulga o normativo a vigorar nas UN e que detém o CCDCM na sua estrutura), da SM/DN (enquanto autoridade técnica dos navios) e da STI/DITIC (enquanto autoridade técnica para as TIC e responsável pelo CORE) e da SP/DF, tendo em vista a elaboração do devido quadro doutrinário e demais normativos, que habilitem a edificação da capacidade de CSC nos navios da Marinha. Assim sendo, as UN passarão a dispor de um quadro normativo adequado, de uma estrutura organizacional, de meios e de pessoal habilitado para reagir e atuar perante ciberataques que possam vir a ocorrer quando as mesmas se encontrarem fora da Base Naval de Lisboa, ou seja, quando as UN estiverem empenhadas num determinado teatro de operações.

Assim, a definição de uma doutrina, a identificação de uma organização a bordo, o estabelecimento dos procedimentos a efetuar consoante as ciberameaças e a formação de pessoal para atuar perante essas situações, irá permitir às UN terem um efetivo conhecimento situacional do ciberespaço de interesse quando as mesmas estiverem empenhadas em missões fora da BNL dotando-as, assim, com capacidade para contribuir para o incremento do seu nível de cibersegurança e assim do da Marinha. Desta forma, considera-se a questão central: ***"O que é necessário existir para que o CSC seja construído nas Unidades Navais e nos Comandos em terra de modo a, num contexto tático e operacional, respetivamente, poder contribuir, de forma atempada, para as tomadas de decisão?"*** e tendo em conta, também, as questões derivadas, a mesma respondida.

Como ideia para um trabalho futuro, sugere-se a densificação das componentes da capacidade de CSC ao nível das UN, designadamente no âmbito da doutrina, do normativo associado ao nível do CN e da matriz de formação atinente, de modo a viabilizar a efetiva edificação da supracitada capacidade.

LISTA BIBLIOGRÁFICA

CEMA, M. F. (2014). *Diretiva de Planeamento da Marinha 2014.* Lisboa: EMA.

CEMA, S. L. (2011). *Directiva de Política Naval 2011.* Lisboa: EMA.

COM(2010)245. (2010). Uma Agenda Digital para a Europa. Bruxelas.

COM(2010)673. (2010). The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Bruxelas.

COM(2012)140. (2012). *Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade.* Bruxelas.

COM(2013)48. (2013). DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Concerning measures to ensure a high common level of network and information*.

COUNCIL OF EUROPE. (2001). Convention on Cybercrime. Budapeste, Hungria.

Decisão 2011/411/PESC DO CONSELHO. (s.d.). Define o estatudo, a sede e as regras de funcionamento da Agência Europeia de Defesa.

ENISA. ([s.d]). Part 2: Policy Recommendations. *Baseline Capabilities National/Governmental CERTs*. [s.l].

EUROPEAN COMMISSION. (6 de julho de 2016). *The Directive on security of network and information systems (NIS Directive)*. Obtido de DIGITAL SINGLE MARKET - Digital Economy & Society: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

EUROPOL. (s.d.). *First Year Report.*

FERNANDES, C. (2014). A dimensão política da Segurança para o ciberespaço na União Europeia. *A Agenda Digital, a Estratégia de Cibersegurança e a cooperação UE - OTAN*.

GEERS, K. (2008). Cyberspace and the changing nature of warfare. *SC Magazine*, 3-5.

GODWIN III, J., KULPIN, A., RAUSCHER, K. F., & YASCHENKO, V. (2014). *The Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2.* Nova Iorque: The EastWest Institute.

Governo de Portugal. ([s.d]). *Multinational Cyber Defence Education & Training*. Obtido de MNCDE&T: http://www.mncdet-pt.net/

Heads of State and Government. ([s.d]). Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. Lisboa.

HEALEY, J., & JORDAN, K. T. (2014). *NATO's Cyber Capabilities: Yesterday, Today and Tomorrow*. [s.l]: Atlantic Council.

IDN. (2013). *Estratégia da Informação e Segurança no Ciberespaço: Investigação conjunta IDN-CESEDEN.* Lisboa: Instituto da Defesa Nacional.

ITU-T. (2008). *Recommendation ITU-T X.1205 - Overview of Cybersecurity.* ITU.

Jorge Valente, M. (2016). Organização da Força Áerea relativamente à cibersegurança. (A. C. COSME, Entrevistador)

MADEIRA, C. R. (2008). O Sistema de planeamento de forças. *Implicações da adopção do Modelo de planeamento por capacidades*.

MARQUES, C. G. (2013). Cibersegurança e Conhecimento Situacional Marítimo. *Revista da Armada*, 13-15.

MARQUES, G. (2013). *Cibersegurança e Conhecimento Situacional Marítimo.* Lisboa: Revista da Armada.

MDN. (2005). *PCA 2 (B) - Doutrina para os sistemas de informação e comunicação automatizados.* Lisboa: EMA.

MDN. (2012). *PCA 16 - Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha.* Lisboa: EMA.

MITRE Corporation. ([s.d]). *Cybersecurity - Situation Awareness*. Obtido em Outubro de 2015, de MITRE: www.mitre.org/capabilities/cybersecurity/situation-awareness

NAC. (2014). Consultation, Command and Control (C3) Board. *NATO Cyber Defence Taxonomy and Definitions*.

NATO. ([s.d]). AD70-1 Parte V INFOSEC. [s.l].

NATO. (2013). *Sharing malware information to defeat cyber attacks*. Obtido de North Atlantic Treaty Organization: http://www.nato.int/cps/en/natolive/news_105485.htm?selectedLocale=en.

NATO. (s.d.). *CCDCOE*. Obtido em 2015, de NATO Cooperative Cyber Defence Centre Of Excellence: https://ccdcoe.org/cyber-definitions.html

NEVES, P. (2014). *Crónica de Tecnologias da Informação e Comunicação, Anais do Clube Militar Naval, Vol. I e Vol. II.* Lisboa: [s.n].

NSA. (2008). *AAP 6 - NATO Glossary of Terms and Definitions.* [s.l]: NATO.

NSA. (2011). *AJP-6 - Allied Joint Doctrine for Communication and Information Systems* . [s.l]: NATO.

OUT-LAW.COM. (2016). *The Network and Information Security Directive – who is in and who is out?* Obtido em Março de 2016, de The Register: http://www.theregister.co.uk/2016/01/07/the_network_and_information_security_directive_who_is_in_and_who_is_out/

PERNIK, P. (2014). *Improving Cyber Security: NATO and the EU.* Tallin: International Centre for Defence Studies.

PINTO, C. N. (2013). Novas fronteiras criadas pelos ciberataques. *Um novo desfio para a cooperação internacional*.

PURSER, S. (2016). Implementig The NIS Directive. Lisboa.

Regulamento (CE) 460/2004. (s.d.).

Republic of Austria. (Março de 2013). *Austrian Cyber Security Strategy.* Viena, Áustria: Federal Chancellery.

REPÚBLICA PORTUGUESA. (2011). Resolução de Conselho de Ministros nº 46/2011. *Diário da República I Série, 218, 14 de novembro de 2011*, 4848.

REPÚBLICA PORTUGUESA. (2012). Resolução do Conselho de Ministros nº 12/2012. *Plano de Ação do GPTIC, Diário da República I Série, 27, 7 de fevereiro de 2012*.

REPÚBLICA PORTUGUESA. (2012). Resolução do Conselho de Ministros nº 42/2012. *Constituição da Comissão Instaladora do Centro Nacional de Cibersegurança, Diário da República I Série, 74, 13 de abril de 2012*.

REPÚBLICA PORTUGUESA. (2013). Despacho n.º 7527-A/2013. *Diretiva Ministerial para a reforma estrutural na Defesa, Diário da República II Série, 111, 11 de junho 2013*.

REPÚBLICA PORTUGUESA. (2013). Despacho nº 13692. *Orientação Política para a ciberdefesa, Diário da República II Série, 208, 28 de outubro de 2013*, 31977-31979.

REPÚBLICA PORTUGUESA. (2014). Decreto-Lei 184/2014. *Lei Orgânica do EMGFA, Diário da República I Série, 250, 29 de dezembro de 2014*.

REPÚBLICA PORTUGUESA. (2014). Decreto-Lei nº 69/2014. *Orgânica do Gabinete Nacional de Segurança, Diário da República I Série, 89, 9 de maio de 2014*.

REPÚBLICA PORTUGUESA. (2015). Decreto-Regulamentar nº 13/2015. *Estrutura do EMGFA, Diário da República I Série, 148, 31 de julho de 2015* .

REPÚBLICA PORTUGUESA. (2015). Resolução do Conselho de Ministros nº 36/2015. *Estratégia Nacional de Segurança do Ciberespaço, Diário da República I Série, 113, 12 de junho de 2015*.

RICHARDS, C. (21 de Março de 2012). *Boyd's OODA Loop (It's Not What You Think).* [s.l]: J. Addams & Partners, Inc.

RIZWAN ALI, C. (2014). *On Cyber Defence.* Obtido em Outubro de 2015, de Joint Warfare Centre: www.jwc.nato.int/images/stories/threeswords/cyber_def_review.pdf

SCHMITT, M. N. (2013). *Tallin Manual on the International Law Applicable to Cyber Warfare.* UK: Cambridge University Press.

TADDA, G. P., & SALERNO, J. S. (2009). Overview of Cyber Situation Awareness. Em *Cyber Situation Awareness* (pp. 15-35). [s.l]: Springer US.

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

UE. (2014). *EU Cyber Defence Policy Framework.* Bruxelas: Council of European Union.

UNIÃO EUROPEIA. (2012). Tratado da União Europeia.

GLOSSÁRIO

Capacidade – É a habilidade para produzir um efeito que é necessário atingir. O efeito é o resultado de uma acção ou conjunto de acções produzidas pela capacidade. Uma capacidade consistirá numa ou mais componentes funcionais: Doutrina, Organização, Treino, Material, Liderança, Pessoal, Facilidades (infra-estruturas) e Interoperabilidade (MADEIRA, 2008).

Ciberameaça – Um perigo que, seja reportado ou detectado, possa originar uma vulnerabilidade cibernética (GODWIN III, KULPIN, RAUSCHER, & YASCHENKO, 2014, p. 38)

Ciberataque – Um ato ou uma ação iniciada no ciberespaço com o intuíto de provocar danos comprometendo as comunicações, a informação ou outros sistemas electrónicos, ou mesmo a informação armazenada, processada ou transmitida através destes mesmos sistemas (NAC, 2014).

Cibercrime – É uma atividade criminal efetuada através do uso de computadores e da *Internet*, frequentemente motivada financeiramente. Inclui roubo de identidade, fraude, golpes na *Internet*, entre outras atividades. Diferencia de outras formas maliciosas de atividades ciber, as quais têm motivações políticas, militares ou de espionagem (NATO, s.d.).

Ciberdefesa – Definido como o conjunto de todas as medidas necessárias à defesa do ciberespaço através de meios militares apropriados para atingir os objetivos estratégicos militares. A ciberdefesa é um sistema integrado, comprometendo a implementação de todas as medidas relacionadas com as TIC e segurança de informação (Republic of Austria, 2013, p. 21).

Ciberespaço – Meio constituído por componentes físicos e não físicos, caracterizado pelo uso de computadores e do espectro electromagnético para armazenar, modificar e partilhar a informação usada nas redes (SCHMITT, 2013).

Ciber evento – Um evento não autorizado e inesperado nos sistemas TIC cujo impacto é mínimo e a sua recuperação é fácil ou automática (NAC, 2014).

Ciberincidente – Um evento não autorizado e inesperado nos sistemas TIC onde as medidas automatizadas falharam e cujo impacto não é grave e a recuperação exige o envolvimento de pessoal especializado (NAC, 2014).

Cibersegurança – Conjunto de ferramentas, de políticas, de conceitos, de orientações, de processos de gestão de risco, de ações, de atividades de treino e prática que, juntamente com as tecnologias, podem ser utilizados para proteger o ciberespaço bem como a organização e os seus meios. Estes incluem os sistemas computacionais, o pessoal, a infraestrutura, os serviços, os sistemas de telecomunicações e toda a informação transmitida e/ou armazenada através do ciberespaço (ITU-T, 2008, pp. 2-3).

Infraestruturas Críticas – Meios e sistemas físicos ou virtuais sob jurisdição de um Estado que são tão essencias/vitais tanto que a sua incapacitação ou destruição poderá debilitar a segurança, a economia, a saúde pública ou o ambiente de um Estado (SCHMITT, 2013, p. 258).