INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO CPOS FA

2016/2017

TII

CONTRIBUTOS PARA A DEFINIÇÃO DAS COMPETÊNCIAS DO CENTRO NACIONAL DE CIBERDEFESA NO PANORAMA DA CIBERSEGURANÇA NACIONAL: A DEFINIÇÃO DE RESPONSABILIDADES E A COORDENAÇÃO COM OS DIFERENTES ATORES

José António Baptista Costa

CAP/TINF

INSTITUTO UNIVERSITÁRIO MILITAR

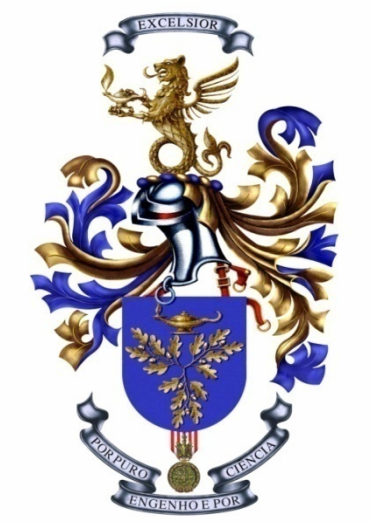
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CONTRIBUTOS PARA A DEFINIÇÃO DAS COMPETÊNCIAS DO CENTRO NACIONAL DE CIBERDEFESA NO PANORAMA DA CIBERSEGURANÇA NACIONAL: A DEFINIÇÃO DE RESPONSABILIDADES E A COORDENAÇÃO COM OS DIFERENTES ATORES

CAP/TINF José António Baptista Costa

Trabalho de Investigação Individual do CPOSFA 2016/2017

Pedrouços 2017



INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CONTRIBUTOS PARA A DEFINIÇÃO DAS COMPETÊNCIAS DO CENTRO NACIONAL DE CIBERDEFESA NO PANORAMA DA CIBERSEGURANÇA NACIONAL: A DEFINIÇÃO DE RESPONSABILIDADES E A COORDENAÇÃO COM OS DIFERENTES ATORES

CAP/TINF José António Baptista Costa

Trabalho de Investigação Individual do CPOSFA 2016/2017

Orientador: **TCOR/ENGAER Susana M. C. P. Abelho**

Pedrouços 2017

Declaração de compromisso Antiplágio

Eu, José António Baptista Costa, declaro por minha honra que o documento intitulado "Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do CPOSFA 2016/2017 no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 26 de junho de 2017

José António Baptista Costa

Assinatura

Agradecimentos

Agradeço:

Ao Major Monteiro da Silva pelas orientações iniciais...

Ao Tenente-Coronel Ralo (Assessor da Direção de Planeamento Estratégico de Defesa) pelo notável contributo e disponibilidade…

Ao pessoal do CCD, principalmente ao Capitão-Tenente Assunção e ao Major Farinha (Coordenadores) pela apresentação do Centro e esclarecimento das questões colocadas…

Ao Capitão-Tenente Baptista das Neves (Chefe do Núcleo CIRC da Marinha),

ao Major Fernandes (Chefe do Núcleo CIRC do Exército),

e ao Major Valente (Chefe do Núcleo CIRC da FAP), pela paciência e tempo dispendido na "colaboração à distancia" e que muito representa neste trabalho…

Ao pessoal do CNCS, ao Professor Pedro Veiga (Coordenador do CNCS), ao Major Raposo (Consultor Coordenador) e ao Major Leite (Jurista), pelo prestável acompanhamento e esclarecimento durante as visitas e entrevistas…

A todos os Docentes pelo conhecimento transmitido que, de forma direta ou indireta, enriqueceu a minha prespetiva sobre este desafio…

A todos os Camaradas do CPOS 2016/2017 pela sã camaradagem…

À minha Orientadora, Tenente-Coronel Susana Abelho, pelo acompanhamento prestado e pelo paciente trabalho de revisão…

Sem a vossa colaboração este trabalho não teria qualquer valor.

À minha esposa Márcia e aos meus filhos Rita e Pedro, que foram a minha grande motivação, a quem dedico todo o meu esforço na superação deste desafio.

A todos, um sincero agradecimento!

Índice

Índice de Figuras

Índice de Tabelas

Resumo

O Centro de Ciberdefesa iniciou a sua operação em 2015 com responsabilidades na ciberdefesa e na cibersegurança setorial da defesa nacional. No decorrer de 2016, a Organização do Tratado do Atlântico Norte e a União Europeia assinaram um Acordo Técnico e uma Declaração Conjunta para reforçar a cooperação no âmbito das operações, exercícios e educação e treino. Nesse mesmo ano, foi aprovada na União Europeia a Diretiva Relativa à Segurança das Redes e da Informação, que será transposta para o ordenamento jurídico nacional até maio de 2018, data que coincide com a revisão da Estratégia Nacional de Segurança do Ciberespaço.

Importa nesta investigação analisar o desenvolvimento da capacidade de atuação da ciberdefesa no ciberespaço nas dimensões de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade, assim como o quadro legal por forma a identificar contributos para o melhoramento da cooperação e coordenação na cibersegurança nacional.

Para tal recorreu-se à estratégia qualitativa, tendo sido utilizado o raciocínio hipotético-dedutivo, a partir de um estudo de caso, a Ciberdefesa nas Forças Armadas.

Esta investigação revela o estado de maturidade da Ciberdefesa e identifica pontos fundamentais de uma futura Estratégia Nacional de Ciberdefesa que permitirá reforçar a sua atuação na cibersegurança.

Palavras-chave

Ciberdefesa, ciberespaço, cibersegurança.

Abstract

The Ciber-defense Center began its operation in 2015 with responsibilities in cyber-defense and sectoral cybersecurity of national defense. During 2016, the North Atlantic Treaty Organization and the European Union signed a Technical Agreement and a Joint Declaration to strengthen cooperation in the field of operations, exercises and education and training. In the same year, the Network and Information Security Directive was approved in the European Union, which will be transposed into the national legal system by May 2018, coinciding with the revision of the National Cyberspace Security Strategy.

It is important to analyze the development of cyber-defense capacity in cyberspace in the dimensions of doctrine, organization, training, material, leadership, personnel, facilities and interoperability, as well as the legal framework in order to identify the contributions for the improvement of cooperation and coordination in national cybersecurity.

For that it was used the qualitative research strategy, trough the hypothetical-deductive reasoning from a case study, the Armed Forces' cyber-defense.

This research reveals the state of maturity of Cyber-defence and identifies key points of a future National Strategy for Cyber-defense that will strengthen its role in cybersecurity.

Keywords

Cyber-defense, cyberspace, cybersecurity.

Lista de abreviaturas, siglas e acrónimos

C

CCD – Centro de Ciberdefesa

CCD COE – *Cooperative Cyber Defence Centre of Excelence*

CEDN – Conceito Estratégico de Defesa Nacional

CERT-EU – *Computer Emergency Response Team for the EU*

CFMTFA – Centro de Formação Militar e Técnica da Força Aérea

CIRC – *Computer Incident Response Capability*

CNCS – Centro Nacional de Cibersegurança

CNPCE – Conselho Nacional do Planeamento Civil de Emergência

CSCS – Conselho Superior de Cibersegurança

CSIRT – *Computer Security Incident Response Team*

CTEN – Capitão-Tenente

D

DIRCSI – Direção de Comunicações e Sistemas de Informação

DOTMLPII – Doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade

DPED – Direção de Planeamento Estratégico de Defesa

E

EMGFA – Estado-Maior-General das Forças Armadas

ENCD – Estratégia Nacional de Ciberdefesa

ENISA – *European Network and Information Security Agency*

ENSC – Estratégia Nacional de Segurança do Ciberespaço

ENSI – Estratégia Nacional de Segurança da Informação

EUA – Estados Unidos da América

F

FAP – Força Aérea Portuguesa

FFAA – Forças Armadas

FOC – *Full Operational Capability*

G

GNS – Gabinete Nacional de Segurança

H

H – Hipótese

I

IC – Infraestruturas Críticas

IDN – Instituto de Defesa Nacional

M

MAJ – Major

MDN – Ministério de Defesa Nacional

MN CD E&T – *Multinational Cyber Defence Education and Training*

N

NATO – North Atlantic Treaty Organization

NCIRC – *NATO Computer Incident Response Capability*

O

OE – Objetivo Específico

OSE – Operadores de Serviços Essenciais

OTAN – Organização do Tratado do Atlântico Norte

P

PCM – Presidência do Conselho de Ministros

PCSD – Política Comum de Segurança e Defesa

PD – Pergunta Derivada

PE – Parlamento Europeu

PP – Pergunta de Partida

PSD – Prestadores de Serviços Digitais

R

RCM – Resolução do Conselho de Ministros

RFA – Regulamento da Força Aérea

S

SRI – Segurança das Redes e da Informação

T

TCOR – Tenente-Coronel

TIC – Tecnologias de Informação e Comunicação

TII – Trabalho de Investigação Individual

U

UE – União Europeia

Introdução

Com a massiva partilha de informação e acesso a serviços a partir da Internet a utilização do ciberespaço generalizou-se atraindo para si muitos utilizadores, alguns deles mal-intencionados capazes de, forma organizada ou não, prejudicar indivíduos, organizações e até Estados, como foi o caso da Estónia em 2007. Deste caso, resultaram lições aprendidas do potencial devastador dos ciberataques sobre infraestruturas críticas[1] (IC) e, assim, passaram a ser identificados como riscos e ameaças prioritárias para os Sistemas de Informação e Comunicação (SIC) que dão suporte ao funcionamento da economia e da sociedade da informação globalizada.

Como resposta à tendência no ambiente de segurança global, houve necessidade de rever o Conceito Estratégico de Defesa Nacional (CEDN), em 2013, o qual preconizou a edificação de uma capacidade de Ciberdefesa nas Forças Armadas (FFAA). Na sequência das orientações da Reforma «Defesa 2020» e das Orientações Politicas de Ciberdefesa traçadas em consonância com o quadro da Política Comum de Segurança e Defesa (PCSD) da União Europeia (UE), em 2014, foi criado um Centro de Ciberdefesa (CCD) integrado na estrutura do Estado-Maior-General das Forças Armadas (EMGFA).

Paralelamente, para concretizar um dos objetivos da consolidação da Estratégia Nacional de Segurança da Informação (ENSI), foi também criado o Centro Nacional de Cibersegurança (CNCS).

A Estratégia Nacional de Segurança do Ciberespaço (ENSC) surgiria apenas em 2015, referindo: "o esforço destinado a reduzir debilidades ao nível da segurança das redes e da informação, aumentando a resiliência das suas infraestruturas críticas, apresenta-se também como fundamental, quer no quadro da União Europeia, ao nível da Estratégia da União Europeia para a Cibersegurança, quer das políticas de Ciberdefesa da Organização do Tratado do Atlântico Norte"(OTAN) (PCM, 2015).

O CCD tem responsabilidades na ciberdefesa nacional e na cibersegurança sectorial da Defesa Nacional em coordenação com os Núcleos *Computer Incident Response Capability* (CIRC) dos Ramos das FFAA. O CNCS, por seu lado, tem responsabilidades de coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, e das IC nacionais.

Atualmente, encontra-se em processo de transposição para o ordenamento jurídico nacional a Diretiva Relativa à Segurança das Redes e da Informação (SRI) aprovada pela

[1] Ver a definição no Apêndice A - Corpo de Conceitos.

UE. O prazo limite destes trabalhos é praticamente coincidente com o prazo máximo de três anos para revisão da ENSC. Importa então aferir que alterações estão previstas às responsabilidades cometidas ao CCD no âmbito da cibersegurança nacional.

Atendendo às limitações temporais disponíveis a esta investigação, pretende-se esclarecer de que forma o CCD, o nosso objeto de estudo, pode melhorar a sua intervenção na cibersegurança nacional em condições normais ou mesmo de estado de emergência.

Para o presente trabalho adotou-se o método de investigação científica, suportado numa estratégia qualitativa recorrendo a um raciocínio hipotético-dedutivo, criado por Karl Popper, a partir de um estudo de caso, a Ciberdefesa nas FFAA.

De modo a garantir um entendimento comum, foi criado um corpo de conceitos que se apresenta no Apêndice A.

O objetivo desta investigação é o de contribuir para a definição de responsabilidades e identificação de como a coordenação do Centro de Ciberdefesa deve ocorrer no domínio da cibersegurança nacional. Complementarmente, estabeleceram- se os seguintes Objetivos Específicos (OE):

OE1 - Verificar a capacidade de atuação da Ciberdefesa no ciberespaço;

OE2 - Identificar contributos para melhoramento da cooperação e coordenação na cibersegurança.

Para alcançar estes objetivos, o investigador abandonou os preconceitos e falsas evidências que condicionam a interpretação da realidade dos factos e elaborou uma pergunta de partida (PP) e duas perguntas derivadas (PD), as principais linhas orientadoras da investigação.

PP: De que forma poderá o CCD melhorar o seu contributo no domínio da cibersegurança nacional?

PD1: Em que nível operacional se encontra a capacidade de ciberdefesa nas FFAA?

PD2: De que forma pode ser melhorada a coordenação entre o CNCS e o CCD?

Tendo como fio condutor a pergunta de partida iniciou-se a exploração pelo estado da arte com abordagens diversificadas através da realização de leituras, entrevistas exploratórias e pausas para reflexão e discussão. Seguiu-se a definição da abordagem e perspetiva teórica para tratar a problemática com a projeção de um modelo "estruturado e coerente, composto por conceitos e hipóteses articulados entre si" (Quivy e Campenhoudt, 2003, p. 115). Na construção do modelo para dar resposta às perguntas derivadas, e

consequentemente à pergunta de partida foram relacionados os conceitos e formuladas as seguintes hipóteses:

H1: A capacidade de ciberdefesa encontra-se em desenvolvimento operacional, ainda com alguns desafios para atingir a *Full Operational Capability* (FOC).

H2: A coordenação das capacidades nacionais de cibersegurança e ciberdefesa deve ser reforçada através dum Plano de Ação conjunto.

A validação empírica destas hipóteses formuladas terá como base a observação e análise da informação recolhida ao longo do trabalho de investigação.

Assim, o presente trabalho, composto por três capítulos começa por apresentar a revisão da literatura e a metodologia seguida. No segundo capítulo é analisado o estado de desenvolvimento da capacidade de ciberdefesa nas FFAA. No terceiro capítulo, exploram-se algumas possibilidades do quadro legal de melhoramento da cooperação entre a ciberdefesa e a cibersegurança. Por último, será apresentada uma síntese retrospetiva de todo o processo de investigação, assim como contributos para o conhecimento, recomendações e sugestões pertinentes para o desenvolvimento de futuras investigações.

1. Revisão da Literatura

O uso generalizado da Internet tornou possível novas formas de comunicação e interação social, económica, política e cultural num espaço globalizado que se denomina por ciberespaço. Este ciberespaço formado pelas infraestruturas físicas e lógicas que sustentam os SIC está vulnerável a ciberameaças que podem ter impacto ao nível económico e social ou até constituir uma ameaça à segurança nacional através da interferência no normal funcionamento das IC nacionais. Por conseguinte, o Estado português tem vindo a implementar medidas no sentido de garantir a livre utilização do ciberespaço, salvaguardando o interesse nacional. Assim, em consonância com as orientações da UE foram criadas duas áreas de segurança e defesa distintas mas complementares, a cibersegurança e a ciberdefesa. A cibersegurança contribui para o uso livre, confiável e seguro do ciberespaço nacional, enquanto que "a ciberdefesa nacional ocupa-se da defesa das infraestruturas críticas nacionais cujo mau funcionamento pode afetar a soberania nacional, atuando dentro e fora do ciberespaço nacional, interagindo com a cibersegurança nacional e com a cibersegurança global" (Ralo, 2016).

Figura nº 1 - Cibersegurança global

Fonte: (Nunes, 2015)

1.1. Ciberdefesa Nacional

Na sequência da revisão do conceito estratégico da OTAN, aprovado em 2010, bem como do novo Tratado da UE (Tratado de Lisboa) a contribuição portuguesa para a garantia da segurança internacional passou a ter novas exigências. Paralelamente, a grave crise económica na Zona Euro, que empurrou Portugal para a assistência financeira internacional, levou à adoção de medidas de austeridade com impacto na segurança e defesa nacional (PCM, 2013a).

Em 2013, a Estratégia da UE para a Cibersegurança, de 7 de fevereiro, estabeleceu como prioridade o desenvolvimento de políticas e capacidades no domínio da Ciberdefesa no quadro da PCSD. Nesse mesmo ano é revisto o CEDN e são aprovadas as linhas orientadoras para uma reforma estrutural na defesa nacional e nas FFAA, designada por Reforma «Defesa 2020»[2] (PCM, 2013b). Posteriormente, seguiu-se a edificação da estrutura de ciberdefesa nacional, no âmbito do EMGFA obedecendo às orientações específicas da Reforma «Defesa 2020» e do Despacho n.º 13692/2013, de 11 de outubro, que apresenta as políticas para a ciberdefesa traçadas em consonância com o quadro da PCSD. Essa edificação teve por base a Orientação para a Política de Ciberdefesa que determinou os princípios essenciais, definiu os seguintes objetivos: "garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques"; "assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional"; e "contribuir de forma cooperativa para a cibersegurança nacional" (MDN, 2013).

A 29 de dezembro de 2014, é criado o CCD através do Decreto-Lei n.º184/2014 que define a nova estrutura orgânica e funcional do EMGFA, a qual prevê a sua integração na Direção de Comunicações e Sistemas de Informação (DIRCSI) (Governo, 2014b). O Decreto Regulamentar 13/2015 viria a elencar para o CCD um conjunto de competências no âmbito da ciberdefesa nacional e da cibersegurança setorial[3] da defesa nacional, que se apresentam no anexo A.

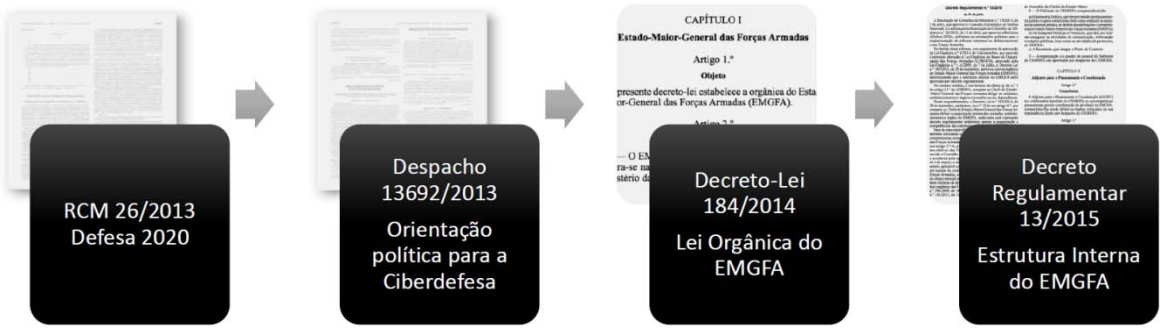


Figura nº 2 - Enquadramento legal da Ciberdefesa

Fonte: (Farinha, 2016)

[2] Aprovado pela Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril.

[3] A cibersegurança setorial engloba todas as redes do Ministério da Defesa Nacional (Assunção, 2016).

1.2. Cibersegurança Nacional

Decorrente do compromisso assumido por Portugal no memorando de entendimento com a Troika[4] em 2011, foi constituído pela Resolução do Conselho de Ministros (RCM) n.º 46/2011, de 14 de novembro, o Grupo de Projeto para as Tecnologias de Informação e Comunicação (TIC), com a missão de elaborar um plano global estratégico de racionalização dos custos suportados pelo Orçamento de Estado com as TIC na Administração Pública (PCM, 2011).

Concluído o Plano de ação é aprovado pela RCM n.º 12/2012, de 12 de janeiro, com cinco grandes eixos de atuação e 25 medidas de racionalização das TIC, das quais se realça a medida quatro que atribui ao Gabinete Nacional de Segurança (GNS) a responsabilidade de coordenar a consolidação da ENSI, em colaboração com todas as entidades relevantes neste âmbito. Um dos vários objetivos nacionais para a segurança da informação previstos na ENSI seria então a criação, instalação e operacionalização de um CNCS (PCM, 2012a).

Para tal materialização, foi constituída uma Comissão Instaladora, através da RCM n.º 42/2012, de 5 de abril, a funcionar na dependência direta do Primeiro-Ministro (PCM, 2012b). Num plano um pouco mais avançado, é aprovada por Decreto Lei nº69/2014, em 9 de maio, uma nova orgânica do GNS que estabelece os termos de funcionamento[5] do CNCS e a sua missão de contribuir para o "uso livre, confiável e seguro do ciberespaço através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional" bem como de ações de combate às ciberameaças que "ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais". Realça-se que o desempenho das competências conferidas ao CNCS (ver anexo B) "não prejudica as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço", nomeadamente as "estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo" (Governo, 2014a).

[4] A Troika foi constituída pelas três entidades: o Fundo Monetário Internacional, o Banco Central Europeu e Comissão Europeia.

[5] O funcionamento do CNCS no âmbito do GNS será objeto de avaliação no final de 2017, com vista a uma decisão sobre a manutenção da dependência ou evolução para uma completa autonomização (Governo, 2014a).

Figura nº 3 – Cibersegurança nacional

Fonte: (Nunes, 2016)

A 7 de outubro de 2014, o CNCS assumiu formalmente as competências referidas no anexo B, relativas ao Estado e às IC (Veiga, 2017).

1.3. Estratégia Nacional de Segurança do Ciberespaço

Na prossecução dos objetivos traçados pelo poder político é aprovada em RCM n.º 36/2015, de 28 de maio 2015, a ENSC que estabelece linhas de ação e objetivos com vista a uma eficaz gestão de crises, a uma resposta operacional a ciberataques, a um desenvolvimento de sinergias nacionais e a uma promoção da cooperação nacional e internacional. Intrincada num vasto quadro legal[6] a ENSC alicerça-se nos pilares da subsidiariedade, da complementaridade, da cooperação, da proporcionalidade e da sensibilização, com vista a aprofundar a segurança do ciberespaço, palco comum de cidadãos, empresas e entidades públicas e privadas. Para além da promoção do uso "consciente, livre, seguro e eficiente do ciberespaço" esta estratégia apresenta outros três objetivos estratégicos: a proteção dos cidadãos no que respeita a direitos fundamentais, liberdade de expressão, dados pessoais e privacidade; o reforço e garantia da "segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais"; e a afirmação do "ciberespaço como um domínio de desenvolvimento económico e de inovação". (PCM, 2015).

[6] "A Estratégia assenta sobre os princípios gerais da soberania do Estado, as linhas gerais da Estratégia da União Europeia para a Cibersegurança e na estrita observância da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa; a Carta dos Direitos Fundamentais da União Europeia, da proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade." (PCM, 2015).

Para reforço do potencial estratégico nacional a ENSC apresenta as orientações gerais e especificas plasmadas em medidas e linhas de ação compartimentadas em seis eixos de intervenção: Eixo 1- Estrutura de segurança do ciberespaço; Eixo 2 - Combate ao cibercrime; Eixo 3 - Proteção do ciberespaço e das infraestruturas; Eixo 4 - Educação, sensibilização e prevenção; Eixo 5 - Investigação e desenvolvimento; Eixo 6 - Cooperação (PCM, 2015).

1.4. Metodologia

Atendendo à natureza do problema a estudar, foi seguido o raciocínio hipotético-dedutivo com recurso a uma estratégia de pesquisa qualitativa. No que diz respeito ao desenho de pesquisa recorreu-se ao estudo de caso, a Ciberdefesa nas FFAA.

Esta investigação teve sete etapas distribuídas por três atos de acordo com a Metodologia de Investigação em Ciências Sociais, proposta por Quivy e Campenhoudt (2005), com a seguinte estrutura:

1.4.1. Rutura

Nesta fase o autor abandonou os preconceitos e as falsas evidências que condicionavam a interpretação da realidade dos factos e percorreu as seguintes etapas:

Etapa 1 – Formulação da PP e PD provisórias[7] que seriam as linhas orientadoras da investigação;

Etapa 2 – Exploração. Tendo como fio condutor as perguntas procedeu-se à revisão da literatura e entrevistas exploratórias a peritos da ciberdefesa[8] intercalando com pausas para reflexão e discussão;

Etapa 3 – Problemática. A problemática foi construída com base no confronto crítico das diferentes perspetivas do problema formulado que se afiguraram possíveis e que iam de encontro às perguntas de partida e derivadas. Esta etapa constitui na charneira para a fase seguinte.

1.4.2. Construção

Ainda a decorrer a etapa da problemática, estruturou-se o modelo de análise (ver apêndice B), composto por conceitos e hipóteses articulados entre si. Seria a etapa 4.

[7] A PP e as PD foram revistas no decorrer da investigação.

[8] CTEN Assunção e MAJ Farinha, oficiais de ligação e analistas do CCD; MAJ Valente, responsável do CIRC da FAP; TCOR Ralo, assessor da DPED; MAJ Leite, jurista e o MAJ Raposo, consultor coordenador, ambos do CNCS.

1.4.3. Verificação

Nesta fase o autor testou a sua proposição pelos factos, nas seguintes etapas:

Etapa 5 – Observação. Nesta etapa foram realizadas entrevistas semiestruturadas a peritos do CCD[9], dos Núcleos CIRC dos Ramos[10] e do CNCS[11] para observar o quê, quem e como (ver apêndices C, D e E);

Etapa 6 – Análise das informações. Refletindo sobre toda a informação recolhida, o investigador validou empiricamente as hipóteses formuladas através da realidade observada. Nesta altura o autor teve necessidade de rever o modelo de análise;

Etapa 7 – Conclusões. Última etapa, na qual realizou-se uma síntese retrospetiva de todo o processo de investigação, assim como a apresentação de contributos para o conhecimento, incluindo recomendações.

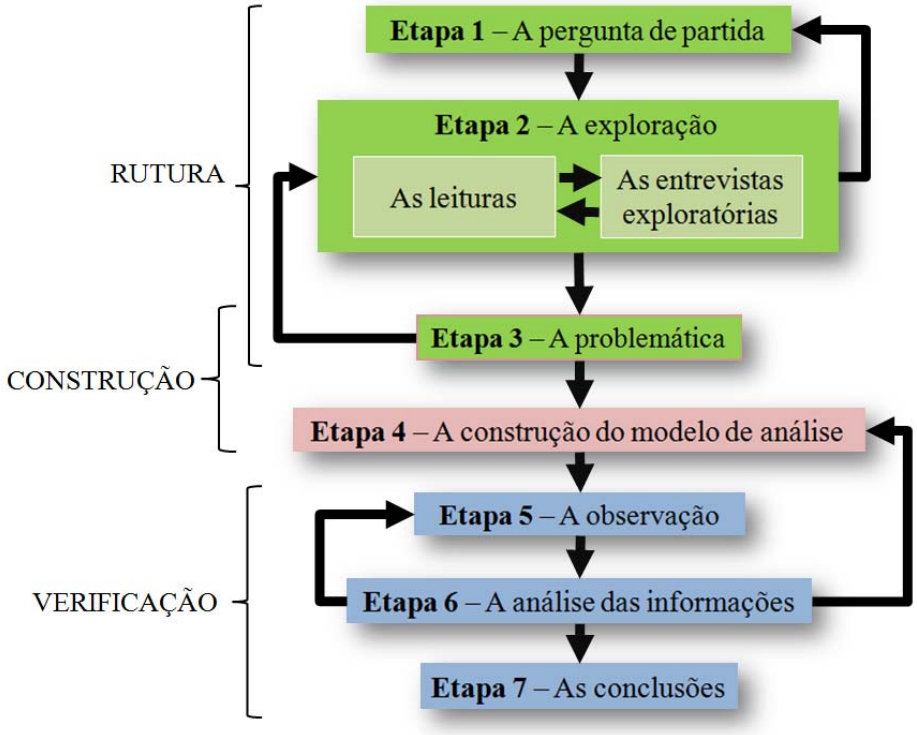


Figura nº 4 – Metodologia de investigação

Fonte: Adaptado (Quivy e Campenhoudt, 2005, p. 27)

[9] CTEN Assunção.
[10] MAJ Valente (FAP), MAJ Fernandes (Exército), CTEN Baptista das Neves (Marinha).
[11] Professor Pedro Veiga e MAJ Leite.

2. Ciberdefesa

A ciberdefesa nacional tem na sua estrutura de comando e controlo o Conselho de Chefes de Estado-Maior que assegura a orientação estratégica-militar e o CCD e os Núcleos CIRC dos Ramos que são responsáveis pelo planeamento e resposta efetiva a uma crise no ciberespaço no âmbito da ciberdefesa e cibersegurança sectorial da defesa nacional (MDN, 2013).

O CCD teve a sua *Initial Operating Capability* em janeiro de 2016, após a implementação de infraestruturas e tecnologias adequadas, investimento em capital humano[12] e criação de procedimentos operacionais. Paralelamente, cada Ramo beneficiou de melhoramento das suas infraestruturas de segurança existentes que passaram a designar-se por Núcleos CIRC e a desenvolver um trabalho colaborativo, integrado e coordenado pelo CCD (Assunção, 2016).

Analisemos o estado de evolução da capacidade militar alcançada pelas FFAA em matéria de ciberdefesa nas componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade (DOTMLPII).

2.1. Doutrina

A doutrina nacional para a ciberdefesa ainda não foi elaborada. O CCD tem como doutrina de referência a "ENSC, a doutrina americana e os planos de acção definidos pela NATO para a condução de operações no ciberespaço" (Assunção, 2017).

A doutrina de ciberdefesa da OTAN[13], embora ainda falte um documento único estruturante (Neves, 2017), deve ser a base para o melhoramento da doutrina nacional (Valente, 2017).

Também as publicações militares de segurança[14] e ciberdefesa deverão ser alvo de atualização e integração de normas e procedimentos necessários para nivelar as idiossincrasias e maximizar a eficácia de cooperação (Neves, 2015). Do ponto de vista da aplicação do direito internacional ao ciberespaço, o Manual de Tallinn é tratado como doutrina, embora seja um documento académico e não vinculativo (CCDCOE, s.d.).

[12] Ao abrigo de uma cooperação com a embaixada dos Estados Unidos da América (EUA) em Portugal, alguns militares do CCD e dos CIRC dos Ramos tem vindo a obter formação na *Nacional Defense University em Washington*, nos EUA (Assunção, 2016).

[13] AC/322-D/0056 "NATO *Computer Incident Response Capability*", AC/322-N/0797 "*NATO Computer Incident Response Capability* (NCIRC) *Concept of Operations*" e o AJP 3.20 "*NATO Doctrine for Cyberspace Operations"* (Draft).

[14] PEMGFA/CSI/301 (EMGFA, 2008), PCA 16 (Marinha, 2012) e RFA 390-6 (FAP, 2011).

2.2. Organização

Com a criação do CCD no EMGFA e dos Núcleos CIRC nos Ramos, "podemos dizer que a organização existe" (Neves, 2017) ainda que, doutrinariamente, não haja qualquer referência concreta a esta "estrutura da ciberdefesa" (Assunção, 2016). De acordo com a Lei Orgânica do EMGFA o CCD assegura "a coordenação e o trabalho colaborativo e integrado com os Núcleos" (Governo, 2014b) que operam localmente ao nível do seu Ramo (Neves, 2016).

Existe um Plano de Edificação da Capacidade de Ciberdefesa que define as responsabilidades de execução de funções críticas de cibersegurança como resposta a incidentes, coordenação, produção de alertas e análise forense (Assunção, 2017). Para cobrir estas responsabilidades o número de recursos humanos existente é muito reduzido (Assunção, 2017), (Neves, 2017), principalmente no Núcleo CIRC do Exército (Fernandes, 2017). Adicionalmente a rotatividade[15] de pessoal, assim como o "custo de formação especializada tornam difícil manter capacidades e qualificações" (Valente, 2017) necessárias no cumprimento da missão.

2.3. Treino

Os exercícios operacionais são eventos por excelência onde o treino permite avaliar e desenvolver tanto a doutrina como identificar lacunas na formação, assim como gerar a partilha e confiança tão necessária à coordenação e cooperação entre os "membros da comunidade ciber" (Neves, 2017). A nível nacional, o Exército tem organizado anualmente, desde 2012, o exercício Ciber Perseu com o objetivo de validar os seus procedimentos e proporcionar o fortalecimento da confiança entre pessoas e instituições (Fernandes, 2017). Na edição de 2016 contou com mais de 50 participantes nacionais entre eles o CCD, os Núcleos CIRC dos Ramos, o CNCS, entre outros (FunchalNotícias, 2016). Já ao nível internacional destaca-se a participação das FFAA (a par do CNCS), como observador no exercício *Locked-shields,* uma iniciativa do *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) (CCDCOE, 2016). Mas é sobretudo no exercício anual de ciberdefesa da OTAN, denominado por *Cyber Coalition*[16], que as FFAA desde

[15] Motivada quer pela progressão na carreira militar, quer pelo tempo máximo de permanência na colocação.

[16] Considerado o maior exercício de ciberdefesa da OTAN com o propósito de treinar a coordenação entre nações.

2011 têm vindo a testar a sua capacidade de ciberdefesa. A última[17] edição, à semelhança das anteriores, decorreu simultaneamente em vários países da OTAN e parceiros com o objetivo de promover a colaboração mútua. De Portugal, reuniram-se no CCD a maioria dos militares da ciberdefesa das FFAA e elementos de "empresas civis, como a Redshift Consulting, a Edisoft, a Fireeye e a Checkpoint que, através dos seus recursos e experiência adquirida na área, colaboraram na resolução dos vários incidentes" (EMGFA, 2016).

Figura nº 5 – Equipa das FFAA no Cyber Coalition 2016

Fonte: (EMGFA, 2016)

O CCD tem vindo a coordenar o trabalho intregado das equipas de Ciberdefesa, sendo a evolução bastante positiva ao nível das "rotinas e procedimentos de resposta" (Assunção, 2017), faltará ainda um exercício nacional conjunto adequado à realidade das FFAA que permita avaliar as capacidades (Valente, 2017).

[17] Realizada entre 29-11-2016 a 1-12-2016, contou com a participação de 28 Estados-membros, mais de 700 militares e civis.

2.4. Material

Desde 2014, o EMGFA tem vindo a equipar os Núcleos CIRC dos Ramos com material para o desempenho das "actividades diárias de detecção, resposta e mitigação de incidentes". No entanto, devido à "grande dispersão territorial" que "aumenta a superfície de ataque exposta, haverá a constante necessidade de manter uma contínua expansão destas ferramentas de monitorização até que se atinja uma total cobertura" (Assunção, 2017).

Esta é provavelmente a dimensão da capacidade mais desenvolvida, mas isso não significa que se deixe de investir continuamente em melhores ferramentas (Fernandes, 2017), como é o caso da necessidade de "uma ferramenta comum de comunicação e partilha de informação sobre os incidentes detetados e que facilite a coordenação da resposta entre os diversos atores" (Neves, 2017).

Valente (2017) considera que embora as tecnologias sejam adequadas ao desempenho da missão, a sua exploração pode ser maximizada com a criação de um conceito de operações.

2.5. Liderança

Os líderes devem conhecer bem as capacidades dos seus membros para fazer a distribuição eficaz das tarefas de resposta aos incidentes de acordo com as suas competências (Neves, 2015). Valente (2017) alerta que essa distribuição de "tarefas com base na especialização sem ter em atenção o posto pode causar desmotivação e perda de coesão nas equipas". O facto de não estar previsto uma carreira ligada à Ciberdefesa deixa a continuidade da participação dos militares nessas equipas sujeita às necessidades de gestão dos recursos humanos, que pode afastar os melhores profissionais. Por isso, esta realidade constitui um desafio à liderança que terá preocupações não só ao nível da formação dos novos elementos, caso se justifique, como também na reorganização das equipas de acordo com as melhores competências (Neves, 2017).

Atualmente, as equipas dos Núcleos CIRC dos Ramos são pequenas e, para Fernandes (2017), não constitui grande preocupação à liderança. No entanto, considera que "a nível macro das Forças Armadas será necessário conjugar todos os esforços de forma a que não se desperdicem recursos escassos a fazer tarefas repetidas". Já para Assunção (2017), o maior desafio tem sido na atribuição de "competências de acordo com a experiência e motivação de cada um", uma vez que se trata de uma área de "grande especialização".

2.6. Pessoal

Para além da necessidade de qualificação adequada a quantidade de recursos humanos é uma clara preocupação (Fernandes, 2017), (Neves, 2017). De acordo com Valente (2017), "se considerarmos todos os aspetos da doutrina de ciberdefesa", no Núcleo CIRC da Força Aérea Portuguesa (FAP) não existem militares suficientes e, mesmo os existentes podem ser empenhados "para tarefas não diretamente relacionadas com a ciberdefesa, prejudicando o tempo disponível para a missão primária". Também no CCD são desempenhadas funções, "nomeadamente nas áreas de estado-maior, para as quais o módulo atual não foi desenhado" (Assunção, 2017).

Para condução de operações no ciberespaço, num regime de horário de trabalho normal, se for necessário o reforço de pessoal no CCD "está prevista a integração de «*augmentees*» provenientes dos CIRC dos três ramos". Se, porventura no futuro, o regime de trabalho de 24/7[18] vier a ser "um requisito operacional, o quadro orgânico do CCD terá que forçosamente ser revisto" (Assunção, 2017). Para isso, "o passo seguinte passará por conseguir identificar pessoal em toda a estrutura das Forças Armadas que possua valências nesta área" (Assunção, 2017) e tenha capacidade "de agir corretamente sobre pressão" (Neves, 2015). Igualmente importante será a valorização deste capital humano que, segundo Neves (2017), "terá de vir de uma carreira que lhes permita evoluir materialmente e ao nivel da formação pessoal".

2.7. Infraestruturas

As infraestruturas são maioritariamente as instalações a partir das quais opera a equipa de resposta a incidentes de ciberdefesa/cibersegurança. Estas devem ser adequadas à preparação e condução das operações, tanto em tempo de paz como em tempo de crise[19] e devem ter como requisitos: a segurança física das instalações através de mecanismos de controlo de acessos e de videovigilância; a segurança lógica dos sistemas de informação e comunicação e provas recolhidas; o fornecimento ininterrupto de energia elétrica e condições ambientais adequadas (Neves, 2015).

Atualmente, com exceção do Núcleo CIRC do Exército existem as infraestruturas operacionais necessárias. Segundo Fernandes (2017), faltará um espaço com requisitos idênticos a uma sala de operações.

[18] Com turnos de 24 horas, sete dias por semana.
[19] Em tempo de crise as infraestruturas devem prever condições para albergar o reforço do efetivo.

2.8. Interoperabilidade

Considerando a natureza complexa e difusa da ciberameaça, assim como o risco de ataques em larga escala, a resposta coordenada e cooperativa ganha eficácia com a interoperabilidade entre os diversos atores privados e públicos, nacionais ou internacionais (Neves, 2015). Na figura seguinte representam-se as ligações de interoperabilidade dentro das FFAA, dentro da rede nacional CSIRT, com a OTAN e com a *European Network and Information Security Agency* (ENISA).

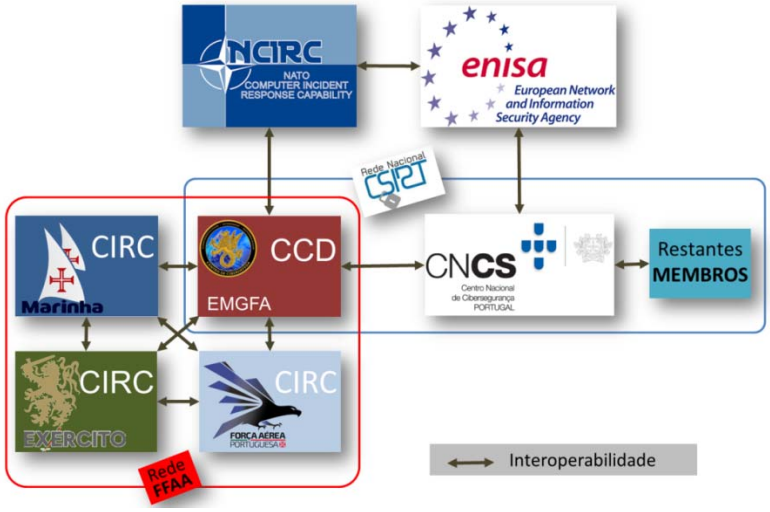


Figura nº 6 - Ligações de interoperabilidade

Fonte: (Autor, 2017)

De realçar que os Núcleos CIRC dos Ramos "não têm a representação junto do fórum CSIRT", apenas o CCD (Valente, 2017).

De acordo com Assunção (2017) tem havido esforços para a utilização de ferramentas, canais de comunicação e procedimentos transversais a toda esta comunidade. Exemplo disso é a partilha[20] entre CCD e o CNCS de informação sobre *malware*[21] na plataforma denominada por *Malware Information Sharing Platform*.

Fernandes (2017) considera que muito embora estejam definidos alguns procedimentos "ainda há muito que evoluir, pois existe alguma relutância das diferentes entidades em partilhar informação", com a implementação de sistemas de informação essa partilha será agilizada.

[20] Esta partilha foi firmada em protocolo pelos dois Centros.

[21] *Software* malicioso como vírus, worms, trojan, keylogger, ransomware, spyware, adware, entre outros.

Face ao exposto, constata-se que todas dimensões têm margem de progressão mas sobretudo as de pessoal, doutrina, liderança e organização que são aquelas que mais validam a H1: "A capacidade de ciberdefesa encontra-se em desenvolvimento operacional, ainda com alguns desafios para atingir a FOC".

Para garantir a cibersegurança sectorial da defesa nacional implica assegurar um vasto leque de competências que "pressupõe a existência de um número de técnicos habilitados a intervir nos vários níveis de ação que permitam uma capacidade de intervenção permanente 24x7". O Núcleo CIRC da Marinha está em fase de qualificação de pessoal e não prevê que a FOC venha a ser atingida num futuro próximo (Neves, 2017). Já Fernandes (2017) refere que no Núcleo CIRC do Exército para cumprir a missão[22] aprovada "ainda estão muitas coisas por definir e operacionalizar" pelo que nem se fala sequer em atingir essa meta. No Núcleo CIRC da FAP, todas as funções definidas em regulamentação própria estão a ser desempenhadas, embora não tenham sido "definidas formalmente quais as condições para atingir a FOC" (Valente, 2017). De acordo com Assunção (2017), concorre para a capacidade de ciberdefesa o desenvolvimento de diversas sub-capacidades que estão em curso, pelo que é prematuro avançar com data concreta para atingir esse objetivo.

A capacidade de ciberdefesa depara-se com alguns desafios e ainda não alcançou o nível operacional desejado para garantir a cibersegurança sectorial da defesa nacional numa situação em que a ciberameaça crie condições de estado de emergência. Assim, considera-se respondida a PD1: "Em que nível operacional se encontra a capacidade de ciberdefesa nas FFAA?".

[22] "A missão aprovada,…, é «prepara-se para executar operações em todo o espectro das operações militares, no âmbito nacional ou internacional, de acordo com a sua natureza. À ordem, integra o Centro de Ciberdefesa…»" (Fernandes, 2017).

3. Cooperação entre Ciberdefesa e Cibersegurança

O Professor Pedro Veiga (2017), Coordenador do CNCS, reconhece que "o CCD tem um conjunto de competências bastante valiosas" e pode contribuir para a cibersegurança nacional quer através do apoio na capacitação do CNCS, quer através da organização de "exercícios de cibersegurança nacionais, de âmbito civil, nos quais se partilhem experiências e se exercite a coordenação numa resposta a ataques". Adianta ainda que, com a transposição da Diretica SRI, o CCD só será chamado a intervir nas IC e Serviços Essenciais civis em situações de estado de emergência, sítio ou guerra, ou então, em situações especiais em que o governo determine a sua intervenção em apoio ao CNCS. Em todo o caso, "a Defesa, nos termos da Constituição, deve-se preparar para eventualmente fazer ataques em casos de conflito, algo que o CNCS não tem mandato e não está preparado" (Veiga, 2017).

Segundo o TCOR Ralo (2016), Assessor na Direção de Planeamento Estratégico de Defesa (DPED), faz parte da agenda digital do Ministro da Defesa Nacional a definição de uma "Estratégia Nacional de Ciberdefesa que consubstancie um Plano de Ação que contribua para o reforço das capacidades nacionais de cibersegurança e ciberdefesa". De acordo com Ralo (2016) e Nunes (2017) esse Plano de Acão deverá conter cinco pontos fundamentais:

- Definição de uma Estrutura de Governação Integrada que possibilite aproximação coerente entre a Cibersegurança e Ciberdefesa;
- Investimento no fator humano através da sensibilização, educação e treino;
- Partilha de informação e conhecimento situacional;
- Investimento em equipamentos e infraestruturas capazes de acompanhar a rápida evolução tecnológica da ciberameaça;
- Cooperação e colaboração nacional e internacional.

3.1. Estrutura de governação integrada

A ENSC refere no "Eixo 1 – Estrutura de segurança do ciberespaço" a definição de "uma coordenação político-estratégica para a segurança do ciberespaço, na dependência directa do Primeiro-Ministro, com representação de todas as partes interessadas", mas que "na prática ainda não está totalmente concretizada" (PCM, 2015). No início do presente

ano, o CNCS fez um conjunto de propostas[23] ao governo, entre elas, a criação de um Conselho Superior de Cibersegurança (CSCS) onde "estejam representados os Ministérios mais relevantes" ao qual "deve competir a coordenação político-estratégica para a segurança e defesa do ciberespaço, assim como dar indicações para o CNCS, para o CCD e para a área do Cibercrime que é gerida pela Polícia Judiciária" (Veiga, 2017).

Este Conselho, caso existisse, deveria também esclarecer uma das competências atribuídas ao CNCS no Decreto-Lei n.º 69/2014, nomeadamente a que consiste em "assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto-Lei n.º 73/2013, de 31 de maio", que, de acordo com Veiga (2017), é uma "ambiguidade", uma vez que o CNCS, com os atuais recursos, não tem essa capacidade nem constitucionalmente tem mandato para tal. Considera que em "situação de guerra" deverá ser o CCD a "liderar o processo e naturalmente os Prestadores de Serviços Essenciais[24] serão obrigados a colaborar".

3.2. Investimento no fator humano

A segurança do ciberespaço depende de uma cultura de segurança promovida juntos dos Utilizadores dos SIC através da sensibilização, educação e treino. Essa cultura já preconizada no "Eixo 4" da ENSC permitirá reduzir a "exposição aos riscos no ciberespaço" e qualificar os recursos humanos colocados no CCD e nos Núcleos CIRC dos Ramos (PCM, 2015).

3.2.1. Sensibilização

De acordo com Neves (2017), na Marinha, "ainda há muito trabalho a desenvolver, nomeadamente ao nível de ações de sensibilização e de pequenos exercícios a desenvolver a nível local, direcionados às comunidades de utilizadores". Devido à escassez de recursos humanos competentes, esse tipo de ações não tem "a frequência e a abrangência que deveriam ter". No Exército, as ações de "*cyber awareness*", como palestras e o exercício anual Ciber Perseu, "fazem parte dos planos e preocupações das pessoas que trabalham estas matérias, pois os utilizadores continuam a ser um elo muito fraco da cadeia da cibersegurança". (Fernandes, 2017). Também na FAP a cultura de segurança é promovida

[23] O CNCS propôs também ao governo que "fosse identificado como a Autoridade Nacional de Cibersegurança, no âmbito da Diretiva SRI e o CSIRT Nacional" (Veiga, 2017).

[24] Entidades das áreas da energia, transportes, saúde ou banca.

"através de aulas no Centro de Formação Militar e Técnica da Força Aérea (CFMTFA), palestras no Curso de Gestão de Matérias Classificadas e palestras solicitadas por algumas Unidades da Força Aérea" (Valente, 2017). No EMGFA, embora tenham sido desenvolvidas algumas acções de sensibilização dos utilizadores, "será necessário apostar de uma forma contínua e persistente para que os resultados se venham a revelar no futuro" (Assunção, 2017).

O CNCS, por seu lado, tem organizado a Conferência Anual de Cibersegurança C-DAYS onde se apresenta e discute a segurança cibernética a nível estratégico, operacional e técnico (CNCS, 2017).

3.2.2. Educação

Para além das inúmeras conferências de ciberdefesa promovidas pelo Exército, Fernandes (2017) defende que a "matéria Ciber deve passar a fazer parte da formação base dos militares". Na FAP, o RFA 390-6 "Política de Ciberdefesa da Força Aérea" de fevereiro desde 2011, já destaca a formação como um pilar fundamental da cultura de segurança e necessária incluir "em todas as estruturas curriculares e em todos os graus de formação administrados na Força Aérea" (FAP, 2011, p. 3-5). No entanto, de acordo com Valente (2017), apenas alguns cursos do CFMTFA são abrangidos.

Em outubro de 2013, Portugal assumiu a liderança do projeto *Multinational Cyber Defence Education and Training* (MN CD E&T), um projeto multinacional de "*Smart Defense*" da OTAN que tem por objetivo "desenvolver/proporcionar novas iniciativas, destinadas a preencher as lacunas de Educação e Treino em Ciberdefesa existentes ao nível da NATO e das Nações" (Exército, 2016). Este projeto, funcionará nas instalações da *NATO Communications and Information Academy*[25], e terá "capacidade para ministrar cursos a um total de seis mil alunos por ano" (Expresso, 2017).

Também iniciativa do projeto MN CD E&T, é a pós-graduação de cibersegurança e ciberdefesa, promovida pela Academia Militar e a Universidade do Minho, que iniciou recentemente, na sua 1ª edição, para ministrar formação avançada a quadros superiores, militares e civis (AM, 2016).

Já o CNCS tem promovido Cursos Gerais de Cibersegurança[26], formações[27] e *workshops*[28] de cibersegurança. (CNCS, 2016).

[25] Atualmente em construção em Oeiras.
[26] Curso destinado aos quadros intermédios e superiores das entidades públicas e privadas.

Figura nº 7 – Iniciativas de educação e treino do Projeto MN CD E&T

Fonte: (Exército, 2016)

3.2.3. Treino

O investimento no fator humano através do treino individual ou coletivo é fundamental. E, exercícios como o Ciber Perseu, o *Locked-shields, o Cyber Europe*[29]*, ou o Cyber Coalition* permitem testar capacidades "em ambiente controlado e identificar lacunas em procedimentos ou ferramentas", assim como estabelecer "relações de confiança" (Valente, 2017).

Os exercícios providenciam "o treino dos processos de apoio à decisão, dos procedimentos técnicos, operacionais e legais relativos à Ciberdefesa, assim como o trabalho colaborativo e de partilha entre os participantes do exercício" (EMGFA, 2016). Para isso, são construídas redes virtuais semelhantes às do mundo real que simulam o estado, a banca e as telecomunicações, entre outros. Ainda é introduzido o papel dos media e da sociedade civil para testar a resposta perante a pressão pública.

O ciberespaço nacional não conhece fronteiras, por isso, todo e qualquer exercício de ciberdefesa ou cibersegurança, de âmbito nacional ou internacional, é uma oportunidade para fortalecer a confiança necessária à cooperação, ganhar proficiência na articulação entre entidades públicas e privadas, assim como para retirar lições apreendidas que mais

[27]Preferencialmente para entidades do Estado, Operadores de Serviços Essenciais e Prestadores de Serviços Digitais.

[28] Destinados a entidades que celebrem protocolos de colaboração com o CNCS.

[29] Exercício bianual de cibersegurança organizado pela ENISA.

tarde podem ter um impato direto na doutrina e nos procedimentos operacionais (Neves, 2015).

3.3. Partilha de informação e conhecimento situacional

Em 2008, criou-se a Rede Nacional de *Computer Security Incident Response Team* (CSIRT) que constitui um "fórum de excelência para a partilha de informação de caráter operacional" (CNCS, 2017). Desde então, entidades das mais variadas áreas como academia, banca, defesa, comunicações, Administração Pública e Operadores IC, entre outras, têm vindo a afiliar-se. Atualmente, conta com os 25 membros representados na figura n.º 7, sendo de realçar a adesão do CCD e do CNCS em 2008 e 2014, respetivamente (CNCS, 2017).

O CNCS tem um papel muito ativo na partilha de informação e conhecimento situacional na rede CSIRT assim como a promoção de um ambiente de cooperação e assistência mútua no tratamento de ciberincidentes. A própria "Diretiva SRI prevê o reforço dessa partilha" (Veiga, 2017).

Embora das FFAA apenas o CCD faça parte dessa rede, é possível ter "acesso a alguns circuitos de informação da rede CSIRT" (Valente, 2017). Segundo opinião de Neves (2017) a partilha dentro das FFAA "tem vindo a aumentar, proporcionalmente ao aumento de confiança existente entre os seus membros", o grande desafio será fortalecer ainda mais essas relações de confiança. Assunção (2017) do CCD refere que "esta partilha de informação e cooperação é essencial para que se consiga um combate eficaz aos ciberincidentes".

Figura nº 8 – Membros da rede nacional CSIRT

Fonte: (CNCS, 2017)

3.4. Investimento em equipamentos e infraestruturas

Perante a crescente frequência e complexidade da ciberameaça, é crucial garantir que as entidades do Estado, os Operadores de Serviços Essenciais (OSE) e os Prestadores de Serviços Digitais[30] (PSD) estejam guarnecidos com equipamentos e infraestruturas para a análise, mitigação e resolução de incidentes de segurança no ciberespaço. Existem diversas soluções no mercado que são por norma dispendiosas, mas também existem ferramentas[31] de *software* livre que são uma boa alternativa.

O investimento em equipamentos e infraestruturas deve ser ajustado às necessidades de segurança e ter profissionais qualificadas para os manusear, assim como procedimentos de cooperação. Nesse sentido, o CNCS concebeu um Modelo de Maturidade de Reação de referência para os atores da cibersegurança, com o objetivo estratégico de assegurar a existência de capacidades técnicas, humanas e processuais. Esse modelo, representado na figura seguinte, apresenta igualmente um plano de desenvolvimento das capacidades encapsuladas em graus de maturidade (Ver anexo C) (CNCS, 2017).

Figura nº 9 – Modelo de maturidade de reação

Fonte: Adaptado (CNCS, 2017)

3.5. Cooperação e colaboração nacional e internacional

A resposta a ciberincidentes transnacionais de larga escala requer uma forte cooperação nacional e internacional quer ao nível estratégico quer ao nível operacional.

[30] Entidades de mercados e motores online e de serviços de computação em nuvem.

[31] O *wireshark* para análise de tráfego, FTK para análise de artefactos e o *cuckoo sandbox* para análise de malware são alguns exemplos.

Por essa razão, a 10 de fevereiro de 2016, a UE e a OTAN assinaram um Acordo Técnico para maior partilha de informação sobre ciberincidentes entre a CERT-EU e a NCIRC. Já durante a Cimeira da OTAN, em Varsóvia na Polónia, em julho de 2016, as mesmas assinaram uma Declaração Conjunta sobre o aumento da cooperação prática em missões e operações, exercícios e educação e treino (EC, 2016). Nesse acordo EU-OTAN foram estabelecidas medidas sobre ciberdefesa e segurança cibernética, com efeito imediato, nomeadamente de interoperabilidade, participação recíproca do pessoal em cursos de formação e nos exercícios como *Cyber Coalition* e *Cyber Europe*, reforço nas ligações entre a UE, a OTAN e o CCDCOE assim como o incentivo à investigação e inovação no domínio da defesa cibernética (CCDCOE, 2017).

Em 9 de maio de 2017, foi assinado um Protocolo de Cooperação entre o GNS/CNCS e o EMGFA/DIRCSI/CCD que visa essencialmente informação sobre as gamas de IP para troca de informação e os pontos de contacto confiáveis.

Figura n.º 10 – Ocasião da Assinatura de Protocolo de Cooperação[32]

Fonte: (EMGFA, 2017)

De acordo com Veiga (2017) "a cooperação e articulação dentro da rede CSIRT nacional inclusive com os CSIRT de entidades privadas tem existido mas é algo que ainda tem de ser melhorado". Também ao nível da celebração de protocolos[33] de cooperação propostos pelo CNCS constata-se um atraso no processo de aprovação pelos diversos

[32] Comodoro Jorge Pires e Professor Pedro Veiga.

[33] Estes protocolos são essenciais para o CNCS se afirmar como o CSIRT nacional. Em maio de 2017, o CNCS apenas tinha protocolos estabelecidos com a EDP e o CCD e em fase de apreciação com a REN e a GALP.

atores sobretudo devido aos "ciclos de tomada de decisão extremamente longos, mesmo das empresas".

Relativamente à Diretiva SRI[34], a "responsabilidade pela coordenação do processo de transposição" foi atribuída à Presidência de Conselho de Ministros (PCM) e ao GNS/CNCS. O CNCS já procedeu a um levantamento das entidades consideradas OSE e dos PSE e tem em curso a elaboração do projeto de ato jurídico que será objeto de consulta pública no segundo semestre do presente ano. Serão tomadas em consideração os contributos de outras entidades, assim como "todos os referenciais necessários", como por exemplo, a ENSC (Leite, 2017).

Os OSE e os PSD serão obrigados a requisitos de segurança e de notificação dos ciberincidentes relevantes para cibersegurança nacional (PE&UE, 2016). De acordo com Leite (2017), as tarefas de fiscalização e auditoria serão atribuídas "às entidades com responsabilidades no modelo de *governance* que será implementado". Adiantou ainda que, "não está prevista qualquer alteração ao âmbito de atuação das Forças Armadas que está preconizado na legislação aplicável".

De uma perspetiva diferente, o reforço das capacidades nacionais de cibersegurança e ciberdefesa poderá ser facilitado pela existência de uma ENCD que consubstancie um Plano de Ação. Neste capítulo, exposeram-se algumas considerações sobre os pontos fundamentais desse futuro Plano de Ação e, dessa forma, validou-se a "**H2**: A coordenação das capacidades nacionais de cibersegurança e ciberdefesa deve ser reforçada através dum Plano de Ação conjunto". Sendo reconhecidas as competências do CCD em matéria de cibersegurança, este Centro pode apoiar na capacitação do CNCS e no planeamento, organização e condução de exercícios de cibersegurança/ciberdefesa à semelhança do que o Exército tem vindo a fazer com o Ciber Perseu. Assim, considera-se respondida a PD2: "De que forma pode ser melhorada a coordenação entre o CNCS e o CCD?".

[34] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho.

Conclusões

Em ciberincidentes de larga escala os Estados e organizações necessitam de cooperar a vários níveis. O CCD tem consagrado no quadro legal um conjunto de responsabilidades ao nível da cibersegurança sectorial da defesa nacional, entre elas a de cooperar com o estruturas nacionais de cibersegurança, nomeadamente com o CNCS.

Dentro dos limites temporais afetos a este trabalho, pretendeu-se esclarecer quais as modalidades de cooperação e articulação entre o CCD e o CNCS para fazer face a uma ciberameaça à soberania nacional que crie condições de estado de emergência e calamidade nacional, como aconteceu na Estónia. Para tal, foi importante aferir, em primeiro lugar, o grau de maturidade da capacidade de ciberdefesa das FFAA, mesmo numa fase tão precoce. Depois, perceber o impacto dos trabalhos de transposição da Diretiva SRI nas responsabilidades do CCD e antever os cinco pontos fundamentais da ENCD que podem contribuir para o reforço das capacidades nacionais de cibersegurança e ciberdefesa. O presente trabalho foi elaborado em torno dessa cooperação assim como da capacidade da ciberdefesa nas FFAA.

Para isso, esta investigação desenrolou-se em sete etapas agrupadas em três fases distintas mas complementares, nomeadamente Rutura, Construção e Verificação. Sem preconceitos e falsas evidências começou-se por formular a PP que serviu de orientação ao trabalho de investigação:

“De que forma poderá o CCD melhorar o seu contributo no domínio da cibersegurança nacional?”

O processo de investigação contou ainda com as linhas orientadoras formuladas nas duas PD que se seguem:

PD1: “Em que nível operacional se encontra a capacidade de ciberdefesa nas FFAA?”

PD2: “De que forma pode ser melhorada a coordenação entre o CNCS e o CCD?”

Na segunda etapa, com o fio condutor das perguntas prossegui-se a exploração através da revisão da literatura e entrevistas a peritos da ciberdefesa. Na fase seguinte, o autor dedicou-se à construção da problemática que seria a charneira entre as fases de Ruptura e Construção. Já na fase de Construção, constituída por uma única etapa, estruturou-se o modelo de análise para sustentar a problemática, formulando-se para validação empírica as seguintes H:

H1: "A capacidade de ciberdefesa encontra-se em desenvolvimento operacional, ainda com alguns desafios para atingir a FOC."

H2: "A coordenação das capacidades nacionais de cibersegurança e ciberdefesa deve ser reforçada através dum Plano de Ação conjunto."

Seguidamente, já na fase de Verificação, na etapa de Observação obteve-se a informação do quê, quem e como através de entrevistas semiestruturadas desta vez a peritos de ciberdefesa e de cibersegurança. Na sexta etapa, procedeu-se à reflexão sobre a informação recolhida e à validação empírica das hipóteses formuladas. Finalmente, na última etapa realizou-se uma síntese retrospetiva do trabalho efetuado, com apresentação de contributos para o conhecimento e recomendações neste capítulo.

Para responder à PP, recorreu-se ao raciocínio hipotético-dedutivo, a partir de um estudo de caso, a Ciberdefesa nas FFAA, utilizando a estratégia qualitativa na análise de legislação OTAN, UE e nacional, assim como de entrevistas a peritos na área da ciberdefesa e cibersegurança.

Relativamente à estrutura do trabalho, no primeiro capítulo foi efetuado um resumo da revisão da literatura, de forma a compreender o estado da arte e os principais conceitos desta investigação, nomeadamente ciberdefesa e cibersegurança nacionais e ENSC. Apresentou-se também a metodologia da investigação, assim como o modelo de análise completo com os conceitos subdivididos em dimensões e indicadores.

No segundo capítulo, foi analisado o estado de desenvolvimento da capacidade de ciberdefesa no CCD e nos Núcleos CIRC dos Ramos nas componentes DOTMLPII, por forma a responder à PD1: "Em que nível operacional se encontra a capacidade de ciberdefesa nas FFAA?". Fez-se a análise dos vários indicadores a partir das respostas às entrevistas semiestruturadas respondidas pelos peritos de ciberdefesa. Verificou-se que todas dimensões da capacidade de ciberdefesa estão num processo evolutivo, umas mais do que outras, sendo que os principais desafios residem nas de pessoal, doutrina, liderança e organização. Desta forma validou-se a H1: "A capacidade de ciberdefesa encontra-se em desenvolvimento operacional, ainda com alguns desafios para atingir a FOC".

No terceiro capítulo procurou-se dar resposta à PD2: "De que forma pode ser melhorada a coordenação entre o CNCS e o CCD?", explorando todas as possibilidades de melhoramento da cooperação entre a ciberdefesa e a cibersegurança. Abordou-se a perspetiva do CNCS no sentido de encontrar convergência de sinergias e antever quaisquer alterações no conjunto de responsabilidades de cibersegurança atribuídas ao CCD, no

âmbito da transposição da Diretiva SRI. Não se vislumbrando quaisquer alterações nesse sentido, explorou-se a cooperação entre a ciberdefesa e a cibersegurança na perspetiva da defesa nacional da DPED, por forma a colher dados sobre o projeto da ENCD. Ainda sem data prevista para aprovação foi adiantada a informação dos cinco pontos fundamentais da Estratégia que podem consubstanciar um Plano de Ação que contribua para o reforço das capacidades nacionais de cibersegurança e ciberdefesa. Assim, explorou-se ponto a ponto com o intuito de apresentar uma possível configuração desse plano, que permite validar a H2: "A coordenação das capacidades nacionais de cibersegurança e ciberdefesa deve ser reforçada através dum Plano de Ação conjunto."

Face ao exposto estamos em condições de responder à PP: "De que forma poderá o CCD melhorar o seu contributo no domínio da cibersegurança nacional?"

Ao nível de pessoal as principais preocupações centram-se na qualificação e quantidade existente de efetivos. Será benéfico para superar tais desidratos a identificação do perfil técnico e dos programas de formação e atualização para funções como as de Coordenador, Analista Forense, Gestor de Incidentes e o Monitor de Eventos. Para além disso, acresce a necessidade de identificar militares com valências técnicas na área de ciberdefesa e capazes de trabalhar em equipa em situações de pressão.

Na interação do CCD e Núcleos CIRC que cooperam para alcançar um objetivo comum torna-se imperativo a elaboração de uma doutrina nacional com base na doutrina OTAN, que defina os objetivos, o âmbito e os princípios fundamentais que permitam a utilização coordenada dos diversos meios.

Sendo a ciberdefesa uma área de intervenção na qual situações de pressão surgem frequentemente, é crucial a existência de equipas coesas, confiantes e motivadas. Por outro lado, a atribuição de tarefas de acordo com a qualificação e não com o posto pode gerar insatisfação que mina o ambiente de trabalho. Assim, os chefes de equipa para além de ter o conhecimento alargado das várias áreas de atuação devem possuir ou desenvolver competências de liderança para comandar, dirigir e motivar os membros da equipa.

Na dimensão Organização, o processo moroso de qualificação, aliado à rotatividade de pessoal motivada pela carreira militar, dificulta a manutenção de capacidades em lidar com a evolução do espectro das ameaças. Para a ciberdefesa, uma área de especial relevo, deve ser criada em cada Ramo das FFAA uma "Bolsa" de militares candidatos a reforçar as equipas de ciberdefesa, de forma permanente ou temporária. Deve ser dada prioridade a

militares com posto compatível com a função e com melhores conhecimentos na área em questão.

A ENSC prevê a coordenação político-estratégica para a segurança e defesa do ciberespaço na dependência direta do Primeiro-Ministro, uma vez que o CNCS está sob a alçada do GNS, que depende da Presidência do Conselho de Ministros, enquanto que o CCD está na dependência do EMGFA, que pertence ao Ministério da Defesa. Essa coordenação não está totalmente concretizada, tendo o CNCS, no início do ano, proposto a criação de um CSC. Perante uma ciberameaça à soberania nacional que crie condições de estado de emergência a existência de uma Estrutura de Governação Integrada permitirá melhorar a articulação entre o CCD e CNCS numa intervenção simultânea. Se se confirmar a criação da EGI na ENCD ela terá a mesma estrutura apenas com nome e agenda diferentes.

Outro ponto da ENCD prende-se com o fator humano que, sendo o elo mais frágil, necessita de sensibilização, formação e treino. À semelhança da Declaração Conjunta assinada pela UE e a OTAN para a cooperação em exercícios, educação e treino, deve o CNCS e/ou o CCD tomar idêntica iniciativa para a realidade nacional. Trata-se de promover a cultura de segurança preconizada pelo "Eixo 4" da ENSC, que permita reduzir "a exposição aos riscos do ciberespaço".

Relativamente à partilha de informação e conhecimento situacional o recente protocolo entre o CCD e o CNCS agiliza o processo. Contudo, os laços de confiança entre as pessoas (técnicos, juristas e outros elementos da cibersegurança) são essenciais e devem ser promovidos.

O investimento em equipamento e infraestruturas é outro ponto da estratégia que, embora não constitua uma preocupação prioritária, deve atender a requisitos de interoperabilidade e uniformização de processos.

Quinto ponto, cooperação e colaboração nacional e internacional como já referido depende dos acordos estabelecidos, mas acima de tudo, dos laços de confiança que se devem promover.

Chegado a esta fase, com base nas opiniões manifestadas pelos peritos é possível tecer as seguintes recomendações e outras considerações de ordem prática para o CCD em coordenação com os Núcleos CIRC dos Ramos:

- Definir etapas com condições para se atingir a FOC;
- Elaborar uma proposta de conteúdo programático de disciplinas de ciberdefesa para os vários graus de conhecimento a ministrar nos cursos de formação dos estabelecimentos de ensino das FFAA;
- Elaborar uma proposta de protocolo de cooperação com o CNCS em exercícios, educação e treino;
- Propor uma doutrina ao nível das FFAA que seja referência nacional que permita a e integração de normas e procedimentos necessários para nivelar as idiossincrasias e maximizar a eficácia de cooperação.

Considera-se ter alcançado os objetivos da investigação ao analisar o estado de maturidade da jovem capacidade de ciberdefesa nas FFAA e ao identificar no quadro legal uma margem de progressão na articulação das sinergias ciberdefesa e cibersegurança. Assim, as FFAA deverão continuar a desenvolver as capacidades no âmbito da ciberdefesa para atingir a FOC e a ENCD ao ser aprovada permitirá consubstanciar um Plano de Ação que facilitará a atuação do CCD na cibersegurança nacional.

A Ciberdefesa em Portugal à semelhança do que acontece em outros países da UE deverá apostar no desenvolvimento contínuo desta capacidade e consequentemente aumento do número de efetivos, assim como no nível de complexidade de resposta através de operações no ciberespaço.

A abordagem deste Trabalho de Investigação não esgotou a temática pelo que existem em aberto caminhos futuros de investigação, como por exemplo:

- Modalidades de cooperação e articulação entre o CCD e o CNCS em estado de sítio;

- Proposta de carreira militar de ciberdefesa;

- Estudo de localização de centro de operações de ciberdefesa alternativo;

- Proposta de qualificação de pessoal destinado a "Bolsa de *Augumentis"* para a Ciberdefesa.

Bibliografia

AM, 2016. *Pós-graduação em cibersegurança e ciberdefesa*. [Em linha] Disponível em: http://academiamilitar.pt/pos-graduacao-em-ciberseguranca-e-ciberdefesa.html [Acedido em 26 de abril de 2017].

MARINHA, 2012. PCA 16: Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha. Lisboa: Marinha.

Assunção, F., 2016. *Exploração da capacidade de ciberdefesa das Forças Armadas* [Entrevista]. Lisboa (17 de novembro de 2016).

Assunção, F., 2017. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (05 de maio de 2017).

CCDCOE, s.d., *Tallinn Manual Process*. [Em linha] Disponível em: https://ccdcoe.org/tallinn-manual.html [Acedido em 28 de fevereiro de 2017].

CCDCOE, 2016. *Locked Shields 2016*. [Em linha] Disponível em: https://ccdcoe.org/locked-shields-2016.html [Acedido em 04 de fevereiro de 2017].

CCDCOE, 2017. *EU-NATO Relations: Hand In Hand Against Cyberattacks*. [Em linha] Disponível em: https://ccdcoe.org/eu-nato-relations-hand-hand-against-cyberattacks.html [Acedido em 04 de fevereiro de 2017].

CNCS, s.d., *CNCS – Glossário*. [Em linha] Disponível em: https://www.cncs.gov.pt/recursos/glossario/ [Acedido em 10 de maio de 2017].

CNCS, 2016. *CNCS - Oferta Formativa*. [Em linha] Disponível em: https://www.cncs.gov.pt/atividades/oferta-formativa/ [Acedido em 10 de dezembro 2016].

CNCS, 2017. *C-Days - Cibersegurança 2017*. [Em linha] Disponível em: https://www.c-days.cncs.gov.pt/ [Acedido em 10 de maio de 2017].

CNCS, 2017a. *Membros da rede nacional de CSIRT*. [Em linha] Disponível em: http://www.cert.rcts.pt/index.php/rede-nacional-csirt/directorio [Acedido em 11 de fevereiro de 2017].

CNCS, 2017b. *Modelo de Maturidade de Reação*. [Em linha] Disponível em: https://www.cncs.gov.pt/certpt/capacitacao-csirt/modelo-de-maturidade-de-reacao/ [Acedido em 11 de fevereiro de 2017].

CNPCE, 2011, *Proteção e Gestão de Risco de Infraestruturas Críticas* [vídeo em linha] Disponível em: http://www.segurancaonline.com/gca/?id=966 [Acedido em 10 de dezembro 2016].

EC, 2016. *NATO summit, Warsaw, Poland, 08-09/07/2016.* [Em linha] Disponível em: http://www.consilium.europa.eu/en/meetings/international-summit/2016/07/08-09/ [Acedido em 29 de janeiro de 2017].

EMGFA, 2008. *PEMGFA/CSI/301: Organização e normas para Resposta a Incidentes de segurança informática nas comunicações e sistemas de informação das Forças Armadas.* Lisboa: EMGFA.

EMGFA, 2016. *Forças Armadas Portuguesas participam em exercício de Ciberdefesa da NATO*. [Em linha] Disponível em: www.emgfa.pt/pt/noticias/1032 [Acedido em 15 de março de 2017].

EMGFA, 2017. *Assinatura de Protocolo de Cooperação entre o Estado-maior General da Forças Armadas e o Gabinete Nacional de Segurança.* [Em linha] Disponível em: http://www.emgfa.pt/pt/noticias/1083 [Acedido em 11 de maio de 2017].

Exército, 2016. *MN CD E&T*. [Em linha] Disponível em: http://www.mncdet-pt.net/ [Acedido em 24 de abril de 2017].

Expresso, 2017. *NATO lança em Oeiras escola para ciberdefesa*. [Em linha] Disponível em: http://expresso.sapo.pt/politica/2017-05-23-NATO-lanca-em-Oeiras-escola-para-ciberdefesa [Acedido em 24 de maio de 2017].

FAP, 2011. *RFA 390-6: Política de Ciberdefesa da Força Aérea.* Lisboa: FAP.

Farinha, J., 2016. *Visão Operacional da Ciberdefesa nas FFAA Portuguesas* [apresentação eletrónica]

Fernandes, P., 2017. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (27 de março de 2017).

FunchalNotícias, 2016. *Madeira treina resposta a ciberataques* [Em linha] Disponível em: https://funchalnoticias.net/2016/11/11/madeira-treina-resposta-a-ciberataques/ [Acedido em 17 de dezembro de 2016].

Governo, 2014a. *Orgânica do Gabinete Nacional de Segurança (Decreto-Lei n.º 69/2014 de 9 de maio)* Lisboa: Diário da República.

Governo, 2014b. *Orgânica do Estado-Maior-General das Forças Armadas (Decreto-Lei n.º 184/2014 de 29 de dezembro)* Lisboa: Diário da República.

IDN, 2013. *Estratégia da informação e segurança no ciberespaço (Caderno nº 12)*. Lisboa: IDN.

IESM, 2015a. *NEP ACA-10 - Trabalhos de Investigação*. Lisboa: IESM.

IESM, 2015b. *NEP ACA-18 – Regras de Apresentação e Referenciação para os trabalhos escritos a realizar no IESM*. Lisboa: IESM.

Leite, A., 2017. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (24 de março de 2017).

MDN, 2013. *Orientações Políticas para a Ciberdefesa (Despacho n.º 13692/2013, de 11 de outubro)* Lisboa: Diário da República.

MDN, 2014. *Diretiva Ministerial de Planeamento de Defesa Militar (Despacho 11400/2014 de 3 de setembro).* Lisboa: Diário da República.

Neves, P., 2015. *Capacidade de Resposta a Incidentes de segurança da informação no Ciberespaço, uma abordagem DOTMLPI-I.* Lisboa: IST.

Neves, P., 2016. *Anais do Clube Militar Naval, Vol. CXLVI, julho-dezembro 2016, p. 781-797, Crónica de Tecnologias da Informação e Comunicação: Ciberdefesa, o Núcleo CIRC da Marinha.* Lisboa: Marinha.

Neves, P., 2017. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (28 de março de 2017).

Nunes, P., 2015, *C-Days 2015 - Sessão 1 - National Cybersecurity Strategies: Staying aligned with future needs* [vídeo em linha] Disponível em: https://www.youtube.com/watch?v=SS2Qsr_Puj4 [Acedido em 9 de dezembro 2016].

Nunes, P., 2015, *1º Curso de Planeamento de Operações no Ciberespaço*. Lisboa: IUM

Nunes, P., 2017, *Conferência "Ciberdefesa: o desafio do século XXI": Contributos para uma Estratégia Nacional de Ciberdefesa. Assembleia da Republica, Sala do Senado, 24 de maio de 2017*. Lisboa: AR.

PCM, 2011. *Constituição do Grupo de Projeto para as Tecnologias de Informação e Comunicação (RCM n.º 46/2011, de 27 de outubro)* Lisboa: Diário da República.

PCM, 2012a. *Plano de ação (RCM n.º 12/2012, de 12 janeiro)* Lisboa: Diário da República.

PCM, 2012b. *Constituição da Comissão Instaladora do Centro Nacional de Cibersegurança (RCM n.º 42/2012, de 5 de abril)* Lisboa: Diário da República.

PCM, 2013a. *Conceito Estratégico de Defesa Nacional (RCM n.º 19/2013, de 21 de março)* Lisboa: Diário da República.

PCM, 2013b. *Reforma «Defesa 2020» (RCM n.º 26/2013, de 11 de abril)* Lisboa: Diário da República.

PCM, 2015. *Estratégia Nacional de Segurança do Ciberespaço (RCM n.º 36/2015, de 28 de maio)* Lisboa: Diário da República.

PE&UE, 2016. *DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO*. [Em linha] Disponível em: http://eur-lex.europa.eu/legal-content /PT/TXT/PDF/?uri=CELEX:32016L1148&from=PT
[Acedido em 10 de dezembro de 2016].

Quivy, R., e Campenhoudt, L.V. (2005). *Manual de Investigação em Ciências Sociais*. 4.ª Edição. Lisboa: Gradiva.

Ralo, J., 2016. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (02 de dezembro de 2016).

Reveron, D.S., 2012. *Cyberspace and national security:threats, opportunities, and power in a virtual world*. Washington, DC: Georgetown University Press.

Valente, A., 2016. *Exploração da capacidade de ciberdefesa das Forças Armadas* [Entrevista]. Lisboa (22 de novembro de 2016).

Valente, A., 2017. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (03 de abril de 2017).

Veiga, P., 2017. *Contributos para a definição das competências do Centro Nacional de Ciberdefesa no panorama da cibersegurança nacional: a definição de responsabilidades e a coordenação com os diferentes autores* [Entrevista]. Lisboa (30 de abril de 2017).

Anexo A — Competências do Centro de Ciberdefesa

(excerto do Decreto Regulamentar n.º 13/2015 de 31 de julho)

“

1 — Ao CCD compete:

a) Assumir a direção e coordenação da capacidade nacional de ciberdefesa, nomeadamente:

i) Conduzir operações militares no ciberespaço;

ii) Garantir a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas;

iii) Elaborar e manter atualizada uma carta de situação do ciberespaço, no domínio das Forças Armadas;

iv) Promover projetos de investigação e desenvolvimento, no âmbito da ciberdefesa;

v) Contribuir para o plano de formação, treino e qualificação dos recursos humanos das Forças Armadas, no âmbito da ciberdefesa;

b) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a ciberdefesa, nomeadamente:

i) Assegurar a capacidade permanente de deteção, resposta e recuperação de ciberincidentes;

ii) Efetuar a análise forense de ciberincidentes;

c) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço, nomeadamente:

i) Contribuir para a elaboração de políticas de segurança no ciberespaço;

ii) Elaborar requisitos de segurança para dispositivos de proteção periférica no ciberespaço;

d) Contribuir para as operações de informação, na vertente Computer Network Operations;

e) Assegurar a coordenação e o trabalho colaborativo e integrado com os núcleos Computer Incident Response Capability (CIRC) dos ramos das Forças Armadas e do EMGFA;

f) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com o Centro Nacional de Cibersegurança e os CIRC nacionais e internacionais;

g) Elaborar e divulgar boletins de segurança com recomendações e contramedidas a implementar em resposta a ameaças emergentes, no âmbito da ciberdefesa;

h) Planear, propor e organizar um programa de exercícios para obtenção de treino;

i) Propor a participação na representação nacional nos organismos nacionais e internacionais, no âmbito da ciberdefesa;

j) Exercer a autoridade técnica no âmbito da ciberdefesa e da cibersegurança setorial da defesa nacional;

k) Reforçar o CCOM, com elementos nomeados em ordem de batalha, quer em operações, quer para a realização de exercícios e treinos, nos planos externo e interno.

2 — No âmbito da cibersegurança setorial da defesa nacional, compete ao CCD:

a) Planear, coordenar e dirigir a investigação de ciberincidentes com relevância para a cibersegurança sectorial da defesa nacional;

b) Estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço;

c) Assegurar a coordenação e o trabalho colaborativo e integrado com os CIRC do universo da defesa nacional;

d) Partilhar a informação numa estratégia de resposta defensiva e colaborativa com os CIRC nacionais e internacionais, de forma articulada com as competências de coordenação da cooperação nacional e internacional do Centro Nacional de Cibersegurança;

e) Cooperar com as estruturas nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.“

Anexo B — Competências do Centro Nacional Cibersegurança

(excerto do Decreto-Lei n.º 69/2014 de 9 de maio)

“

1 — Na prossecução da sua missão, o CNCSeg possui as seguintes competências:

a) Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;

b) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;

c) Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;

d) Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;

e) Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;

f) Assegurar a produção de referenciais normativos em matéria de cibersegurança;

g) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;

h) Assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência, no quadro definido pelo Decreto Lei n.º 73/2013, de 31 de maio;

i) Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;

j) Exercer as demais competências que lhe sejam atribuídas por lei.”

Anexo C — Modelo de Maturidade de Resposta

Tabela nº Anx C-1 – Modelo de Maturidade de Resposta (CNCS, 2017)**.**

FASE	CAPACIDADES
Preparação (Maturidade 1)	• Tenha definido um ponto de contato e articule com o CNCS a reação a incidentes de cibersegurança. • Tenha identificadas as áreas de atividade e serviços considerados críticos ou vitais e realize gestão de ativos para as mesmas.
Técnica (Maturidade 2)	• Colete e armazene metadados de comunicações electrónicas e outros registos de serviços informáticos necessários para a análise de incidentes. • Possua um conjunto de instrumentos técnicos e serviços, autónomos ou contratados, para mitigação dos tipos de ciberataques mais comuns.
Humana (Maturidade 3)	• Possua os recursos humanos com as competências necessárias para realizar grande parte das investigações forenses necessárias e articule com eficácia com o CNCS.
Processual (Maturidade 4)	• Tenha aprovados e implementados procedimentos internos de resposta a incidentes de cibersegurança. • Tenha definida a estrutura e a cadeia de responsabilidade nesta matéria e realize, periodicamente, simulacros de cibersegurança.
Organizacional (Maturidade 5)	• Possua uma equipa dedicada à reação a incidentes de cibersegurança – CSIRT. • Colabore em projetos de desenvolvimento e partilhe informação de cibersegurança de uma forma regular dentro da comunidade nacional de CSIRT. • Participe em exercícios nacionais e internacionais de cibersegurança.

Apêndice A – Corpo de conceitos

- Ciberdefesa Nacional: "…aplicação de medidas de segurança para a proteção e resposta a ciberataques lançados contra infraestruturas TIC, requerendo uma capacidade de preparação, prevenção, deteção, resposta, recuperação e extração de lições aprendidas a partir dos ataques que podem afetar a confidencialidade, integridade e disponibilidade da informação, assim como os recursos e serviços dos sistemas de TIC que a processam" (NC3A, s.d. cit. por IDN, 2013, p.35). É uma **capacidade militar**[35] formada pelas capacidades do CCD e dos Núcleos CIRC dos Ramos das FFAA, que opera no **ciberespaço**[36] contra a **ciberameaça**[37].

- Cibersegurança Nacional: Conjunto de medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou **ciberataques**[38], ponham em causa o funcionamento dos organismos do estado, das **infraestruturas críticas**[39] e dos interesses nacionais (CNCS, 2014). É a capacidade resultante das ações desenvolvidas subsidiariamente e da cooperação na Rede Nacional CSIRT pelas várias entidades civis ou militares, publicas ou privadas para manutenção da segurança no ciberespaço nacional.

[35] Capacidade militar é o "conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade" (MDN, 2014).

[36] Ciberespaço é o "…domínio global no ambiente de informação que consiste em infraestruturas de redes de tecnologia de informação interdependentes (incluindo internet), redes de telecomunicações, sistemas de computadores e controladores e processadores" (US DoD cit. por Reveron, 2012, p.5).

[37] Ciberameaça é qualquer circunstância ou evento passível de explorar, intencionalmente ou não, uma vulnerabilidade específica num sistema de TIC, resultando numa perda de confidencialidade, integridade e disponibilidade da informação manipulada ou da integridade ou disponibilidade do Sistema" (IDN, 2013, p. 22).

[38] "É uma das formas que pode tomar a Ciberguerra. Poderá ser combinada com um ataque físico ou não, e destina-se a provocar danos na capacidade dos sistemas" (FAP, 2011, p. 1-3).

[39] Considera-se IC, "aquela cuja destruição total ou parcial, disfunção ou utilização indevida possa afetar, direta ou indiretamente, de forma permanente ou prolongada" afetar o bem-estar social e a soberania social (CNPCE, 2011).

Apêndice B – Mapa Concetual

Tabela n.º Apd B-1 – Mapa conceptual

Pergunta de Partida	Perguntas Derivadas	Hipóteses	Conceitos	Dimensões	Indicadores
PP: De que forma poderá o CCD melhorar o seu contributo no domínio da cibersegurança nacional?	**PD1**: Em que nível operacional se encontra a capacidade de ciberdefesa nas FFAA?	**H1:** A capacidade de ciberdefesa encontra-se em desenvolvimento operacional, ainda com alguns desafios para atingir a FOC.	Ciberdefesa Nacional	Capacidade	Doutrina
					Organização
					Treino
					Material
					Liderança
					Pessoal
					Infraestruturas
					Interoperabilidade
	PD2: De que forma pode ser melhorada a coordenação entre o CNCS e o CCD?	**H2:** A coordenação das capacidades nacionais de cibersegurança e ciberdefesa deve ser reforçada através dum Plano de Ação.	Cibersegurança Nacional	Quadro legal	Governance
				Cultura de segurança	Sensibilização
					Educação
					Treino
				Capacidade	Partilha de informação
					Investimento em equipamentos e infraestruturas
					Cooperação
					Maturidade

Apêndice C – Análise de entrevistas no EMGFA e nos Ramos

Tabela n.º Apd C-1 – Análise de entrevistas no EMGFA e nos Ramos

INDICADOR	EMGFA(CTEN Assunção), MARINHA (CTEN Baptista das Neves), EXÉRCITO (MAJ Fernandes) FORÇA AÉREA (MAJ Valente)
DOUTRINA	**1. A doutrina (NATO, EU, nacional, sectorial, outra) existente é adequada? De que forma pode ser melhorada?** **EMGFA**: "…ainda não existe doutrina nacional para a Ciberdefesa, sendo a nossa referência, em primeiro lugar, a estratégia nacional para a segurança do ciberespaço, a doutrina americana e os planos de acção definidos pela NATO para a condução de operações no ciberespaço…" **MARINHA**: "A nível nacional o campo doutrinário encontra-se ainda muito deficitário, refletindo-se esta falta de Doutrina fundamentalmente em lacunas procedimentais,…, quais as dependências funcionais e hierárquicas entre órgãos,…,estrutura (Ciberdefesa) não se encontra enquadrada,…,inexistência de uma Estratégia Nacional de Defesa para o Ciberespaço e uma Estratégia de Ciberdefesa,…, (NATO) falta ainda um documento único estruturante,…, (EU) orientações ou melhores práticas, mas também ainda não conheço a Doutrina de Cibersegurança comum…" **EXÉRCITO**: "…praticamente não existe doutrina na área. O AJP 3.20 *NATO Doctrine for Cyberspace Operations* parece que ainda nem sequer saiu. No contexto nacional também é necessário definir bem o modo articulação das diferentes entidades que tratam destas matérias…" **FORÇA AÉREA**: "…a doutrina existente na NATO é adequada,…, doutrina nacional pode e deve ser melhorada tendo como base a doutrina da NATO, mas sendo adaptada à realidade nacional."
ORGANIZAÇÃO	**2. Os recursos humanos estão organizados em equipas de trabalho multidisciplinares e desempenham exclusivamente as funções críticas de cibersegurança como resposta a incidentes, coordenação, produção de alertas e análise forense? Quais são os principais desafios?** **EMGFA**: "Sim. Apesar de serem em número reduzido,…, De acordo com o definido no Plano de Edificação da Capacidade de Ciberdefesa, os CIRC (Computer Incident Response Capability) dos ramos e da Defesa, têm a responsabilidade de execução das funções críticas que descreveu, e neste momento estão dotados com os sistemas adequados para o fazerem,…, O principal desafio neste momento prende-se com a formação destes recursos humanos, a formação de militares para a condução de operações no ciberespaço é um processo moroso e continuado, requerendo uma atenção permanente da evolução do espectro das ameaças por forma a poder detectar, responder e mitigar os diversos incidentes." **MARINHA**: "…com a criação do Centro de Ciberdefesa e dos Núcleos CIRC nos Ramos por parte dos militares e do Centro de Cibersegurança pelo Governo, podemos dizer que a organização existe,…, problema relacionado com os recursos humanos está diretamente ligado ao seu número, claramente insuficiente e sem as qualificações adequadas para assegurar as necessidades do país,…, desafio será,…, decidir investir na formação e alocação de recursos humanos que possam assegurar as necessárias ações de Cibersegurança e de Ciberdefesa." **EXÉRCITO**: "…os recursos humanos escasseiam na generalidade das áreas. Nesta concretamente são mesmo escassos! E as competências em termos formativos nesta área são elevadas e ainda não dispomos delas. Será necessário uma clara aposta na formação de recursos humanos especializados na área." **FORÇA AÉREA**: "Um dos principais desafios desta área é a qualificação do pessoal. A rotação de pessoal, os novos desafios nesta área e o custo de formação especializada tornam difícil manter capacidades e qualificações. Outro dos desafios é a organização interna da capacidade de ciberdefesa e a sua articulação com os restantes serviços de TI."
TREINO	**3. A participação dos recursos humanos em exercícios de âmbito interno, nacional ou internacional tem permitido a validação de procedimentos e doutrina, identificação de lições, assim como o reforço das relações de confiança? Caso de justifique, quais os principais aspetos a melhorar?** **EMGFA**: "… Desde 2015 esta participação tem vindo a ser coordenada directamente pelo CCD com vista a trabalhar cada vez mais a questão dos procedimentos integrados entre as equipas, quer internamente, quer com entidades externas, sendo que esta tarefa está cometida em exclusivo ao CCD,…, A evolução tem sido bastante positiva, permitindo criar rotinas e procedimentos de resposta adequados." **MARINHA**: "…O grande produto do ciberexercícios tem sido a construção das fundamentais relações de confiança entre os membros da comunidade ciber (militares e civis)"; "permitem identificar as nossas lacunas de Doutrina e Formação…" **EXÉRCITO**: "Quando as competências são diminutas qualquer possibilidade de incremento destas é uma mais-valia. E sem duvidas que a participação em exercícios se constitui como fulcral no desenvolvimento da capacidade Ciber,…, (Exercício Ciber Perseu) o relacionamento entre as pessoas e as instituições que tem sido conseguido é apontado como uma grande valia do exercício." **FORÇA AÉREA**: "A participação dos recursos humanos em exercícios permite testar a nossa capacidade em ambiente controlado e identificar lacunas em procedimentos ou ferramentas. Nos exercícios conjuntos, o estabelecimento de relações de confiança entre os elementos especialistas dos vários Ramos,…, a melhorar é a criação de um exercício conjunto mais adequado à nossa realidade."

MATERIAL	**4. Estão disponíveis tecnologias e sistemas de informação e comunicação adequados para o desempenho de atividades de análise de tráfego de rede, resposta a incidentes bem como a análise forense de artefactos? Caso se justifique, quais as principais necessidades?** **EMGFA**: "O CCD tem vindo, desde 2014, a equipar a Capacidade de Ciberdefesa das FFAA com as ferramentas e meios materiais necessários à condução das actividades diárias de detecção, resposta e mitigação de incidentes,…, Face à grande dispersão territorial, que por sua vez aumenta a superfície de ataque exposta, haverá a constante necessidade de manter uma contínua expansão destas ferramentas de monitorização até que se atinja uma total cobertura…" **MARINHA**:: "…faltará encontrar uma ferramenta comum de comunicação e partilha de informação sobre os incidentes detetados e que facilite a coordenação da resposta entre os diversos atores…" **EXÉRCITO**: "…já dispomos de algumas ferramentas adequadas, mas vai ser necessário continuar a investir nesta área…" **FORÇA AÉREA**: "…tecnologias adequadas ao desempenho das missões associadas à ciberdefesa existem após alguns investimentos do Centro de Ciberdefesa do EMGFA,…, principal dificuldade em relação ao uso destas ferramentas é a criação de um conceito de operações que permita tirar partido pleno de todas as capacidade que as ferramentas disponibilizam…"
LIDERANÇA	**5. É promovida a coesão, confiança e motivação dos recursos humanos, afetando-lhe tarefas de acordo com as suas competências? Quais as principais preocupações na liderança de equipas?** **EMGFA**: "…o desenvolvimento das capacidades humanas,…, tem sido um desafio no sentido de atribuir as competências de acordo com a experiência e motivação de cada um,…, o curto quadro orgânico não nos possibilita uma distribuição estanque das competências a formar e treinar, pelo que tem este é um dos principais desafios com que nos defrontamos uma vez que esta é uma área que obriga a uma grande especialização…" **MARINHA**: "…não está prevista uma carreira ligada à Ciberdefesa,…, frequente as necessidades de gestão de carreira afastar os melhores profissionais…" **EXÉRCITO**: "…as equipas são muito pequenas pelo que não implica atualmente grandes preocupações de liderança nessa equipas,…, a nível macro das Forças Armadas será necessário conjugar todos os esforços de forma a que não se desperdiçam recursos escassos a fazer tarefas repetidas nos vários ramos das Forças Armadas." **FORÇA AÉREA**: "…Atribuir tarefas com base na especialização sem ter em atenção o posto pode causar desmotivação e perda de coesão nas equipas…"
PESSOAL	**6. Existem recursos humanos bem formados e treinados, assim como em número suficiente, para fazer face às multiplas tarefas desempenhadas em operações defensivas e/ou ofensivas quer em tempo de paz quer em tempo de crise (regime de trabalho 24/7)? Quais os principais desafios na valorização do capital humano?** **EMGFA**: "…o módulo fixo do CCD é suficiente para as operações diárias atuais, num regime de horário de trabalho normal,…, O treino e a formação são processos evolutivos e contínuos,…, os recursos humanos atribuídos à Capacidade de Ciberdefesa estão bastante melhor formados e treinados do que no dia em que se apresentaram nestas funções,…, Não está previsto nesta fase a adopção de um regime de trabalho de 24/7, sendo que na data em que seja um requisito operacional, o quadro orgânico do CCD terá que forçosamente ser revisto,…, há outras funções a desempenhar, nomeadamente nas áreas de estado-maior, para as quais o módulo atual não foi desenhado,…, condução de operações no ciberespaço que requeiram um número maior de elementos, está prevista a integração de "augmentees" provenientes dos CIRC dos três ramos,…, conseguir identificar pessoal em toda a estrutura das Forças Armadas que possua valências nesta área…" **MARINHA**: "Reforço a ideia de serem necessários mais recursos, com a formação adequada,…, A valorização terá de vir de uma carreira que lhes permita evoluir materialmente e ao nivel da formação pessoal (académica)…" **EXÉRCITO**: "Não. Claramente não!.., o maior problema relacionado com os recursos humanos está diretamente ligado ao seu número, claramente insuficiente e sem as qualificações adequadas para assegurar as necessidades do país,…, Os desafios passam pela formação de novas pessoas em cursos que agora começam a aparecer, como por exemplo a Pós-Graduação em Cibersegurança e Ciberdefesa promovida no âmbito do projeto Multinational Cyber Defence Education and Training Project (MN CD E&T) e outros de natureza mais técnica…" **FORÇA AÉREA**: "…Se considerarmos todos os aspetos da doutrina de ciberdefesa, considero que não existem recursos humanos suficientes,…, o uso dos recursos humanos para tarefas não diretamente relacionadas com a ciberdefesa, prejudicando o tempo disponível para a missão primária…"
INFRAESTRUTURAS	**7. Existem infraestruturas adequadas em termos de segurança, ambiente e usabilidade que permitam a condução de operações em tempo de paz ou de crise? Se houver necessidade de melhoramento, quais os principais requisitos em termos de infraestruturas?** **EMGFA**: "…As limitações existentes nas infraestruturas têm vindo a ser colmatadas com os investimentos realizados desde 2014, pelo que não se considera existirem limitações atuais neste campo…" **MARINHA**: "…Atualmente quer o Centro de Ciberdefesa quer os Núcleos CIRC dos Ramos já possuem estas infraestruturas operacionais…" **EXÉRCITO**: "No caso do Exército ainda não estão disponíveis as infraestruturas mais adequadas. Os requisitos são semelhantes a uma normal sala de operações..." **FORÇA AÉREA**: "Existem infraestruturas adequadas e suficientes para a condução de operações de ciberdefesa…"

INTEROPERABILIDADE	8. **Existem ferramentas, canais e procedimentos de comunicação interoperáveis, bem como protocolos, para partilha de informação de forma eficaz, usando uma taxonomia comum, na rede de CSIRT nacional e internacional (caso se aplique)? Quais os principais aspetos a melhorar?** **EMGFA**: "A comunidade de interesse no domínio do ciberespaço é bastante heterogénea e os interesses principais de cada um diferem de área para área, no entanto têm sido desenvolvidos esforços para a utilização de ferramentas, a criação de canais de comunicação e de procedimentos que sejam transversais a toda esta comunidade,…, o CCD e o CNCS firmaram recentemente um protocolo que servirá de base à edificação da infraestrutura da plataforma para partilha de informação sobre malware (Malware Information Sharing Platform)…" **MARINHA**: "…existe de facto uma estreita relação dentro da comunidade nacional de CSIRT,…, Está a ser feito um esforço conjunto de adoção de uma Taxonomia comum…" **EXÉRCITO**: "…Existem alguns procedimentos definidos. Mas ainda há muito que evoluir, pois existe alguma relutância das diferentes entidades em partilhar informação,…, em implementação sistemas de informação que vão agilizar esta partilha…" **FORÇA AÉREA**: "…os Ramos não têm a representação junto do fórum CSIRT…"
DOLMLPII	**9. Quais das dimensões da capacidade de ciberdefesa/cibersegurança, nomeadamente doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade se encontram melhor desenvolvidas e quais carecem de maior atenção?** **EMGFA**: "…mais desenvolvidas serão as das áreas de material e treino. Desde 2014 o CCD tem vindo a concretizar o projecto de edificação de plataformas de monitorização das infra-estruturas CSI das FFAA's, apresentando nesta fase uma boa maturidade no que respeita à monitorização, detecção e mitigação de incidentes. No que respeita ao treino, as FFAA's, por intermédio dos ramos e coordenação do EMGFA, participam em exercícios de ciber desde 2011, com a edificação do CCD esta participação intensificou-se estando representados anualmente em três exercícios a nível NATO e um a nível nacional. A área que carece de maior atenção e empenhamento é a da doutrina e procedimentos…" **MARINHA**: "…ao nível da Doutrina, Liderança e Pessoal que existem as maiores lacunas…" **EXÉRCITO**: "…mais desenvolvidas,…, talvez as infraestruturas e interoperabilidade,…, que carecem de maior atenção realço a doutrina e organização, além questão do pessoal…" **FORÇA AÉREA**: "…Mais desenvolvidas: infraestruturas, material. Menos desenvolvidas: Pessoal, doutrina e organização..."
CULTURA DE SEGURANÇA	**10. Tem sido promovida uma cultura de segurança aos demais utilizadores? Quais tem sido as principais ações e qual o feedback recebido?** **EMGFA**: "O utilizador comum ,…, é sem dúvida o elo mais,…, Têm sido desenvolvidas algumas acções de sensibilização dos utilizadores no entanto, considero que esta seja uma área em que será necessário apostar de uma forma contínua e persistente para que os resultados se venham a revelar no futuro." **MARINHA**: **"**Atualmente o maior risco de segurança aos sistemas informáticos está diretamente ligado à exploração de vulnerabilidades que resultam de comportamentos de risco por parte dos seus utilizadores,…, ainda muito trabalho a desenvolver, nomeadamente ao nível de ações de sensibilização e de pequenos exercícios a desenvolver a nível local, direcionados às comunidades de utilizadores,…, o insuficiente número de quadros técnicos competentes não tem permitido a realização destas ações com a frequência e a abrangência que deveriam ter…" **EXÉRCITO**: "Ações de cyber awareness fazem parte dos planos e preocupações das pessoas que trabalham estas matérias, pois os utilizadores continuam a ser um elo muito fraco da cadeia da cibersegurança,…, Têm sido desenvolvidas algumas ações, nomeadamente palestras e no próprio exercício Ciber Perseu, em que por exemplo é enviado um e-mail de phishing aos utilizadores do Exercício para nos apercebermos da sensibilidade para este vetor de ataque e treinar esses utilizadores por forma a mitigar ataques reais,…, Considero que matéria Ciber deve passar a fazer parte da formação base dos militares." **FORÇA AÉREA**: "Faz parte da missão das equipas de ciberdefesa, a promoção da cultura de segurança da Organização,…, esta promoção (de cultura) é efetuada através de aulas no CFMTFA, palestras no Curso de Gestão de Matérias Classificadas, e palestras solicitadas por algumas Unidades da Força Aérea…"
PARTILHA	**11. Tem havido partilha de informação e conhecimento situacional na rede CSIRT que promova um ambiente de cooperação e assistência mútua no tratamento de ciberincidentes? Quais os principais desafios?** **EMGFA**: "Sim, esta partilha de informação e cooperação é essencial para que se consiga um combate eficaz aos ciberincidentes." **MARINHA**: "…a partilha de informação tem vindo a aumentar, proporcionalmente ao aumento de confiança existente entre os seus membros,…, o desafio consiste em aumentar precisamente as relações de confiança entre os membros…" **EXÉRCITO**: "…É o EMGFA que faz parte da rede CSIRT, o Exército atualmente não integra individualmente essa rede..." **FORÇA AÉREA**:"…Apesar de não ter assento na estrutura CSIRT nacional, a Força Aérea tem acesso a alguns circuitos de informação da rede CSIRT o que permite afirmar que existe partilha de informação e conhecimento situacionais…"

MATURIDADE	**12. Está previsto o Centro/Núcleo/Secção vir a atingir a *Full Operational Capability* num futuro próximo? Quais as principais condições a alcançar?** **EMGFA**: "A edificação da capacidade de ciberdefesa é um processo em curso composto pelo desenvolvimento de diversas sub-capacidades. É prematuro neste momento poder avançar em concreto com uma data para atingir a FOC." **MARINHA**: "…a Full Operacional Capability pressupõe a existência de um número de técnicos habilitados a intervir nos vários níveis de ação que permitam uma capacidade de intervenção permanente 24x7,…, Apesar de já existir algum pessoal em formação, não se prevê que a FOC venha a ser atingida num «futuro *próximo*»…" **EXÉRCITO**: "…Ainda estão muitas coisas por definir e operacionalizar pelo que não se fala sequer em atingir a FOC,…, A missão aprovada do Núcleo CIRC (Computer Incident Response Capability) do Exército (NuclCIRCEx), é «prepara-se para executar operações em todo o espectro das operações militares, no âmbito nacional ou internacional, de acordo com a sua natureza. À ordem, integra o Centro de Ciberdefesa do Estado-Maior-General das Forças Armadas (EMGFA)»." **FORÇA AÉREA**: "Em relação às funções definidas para a Secção de Ciberdefesa da DCSI na Força Aérea em regulamentação própria, todas elas já estão a ser desempenhadas,…, Em relação ao núcleo CIRC da Força Aérea, não foram definidas formalmente quais as condições para atingir a FOC. No entanto continuam os trabalhos no sentido de melhorar a capacidade e a eficácia do núcleo CIRC da Força Aérea".
OUTROS	13. **Que outro assunto considera pertinente que possa reforçar a cooperação e articulação para o melhoramento da cibersegurança que não tenha sido focado**? **EMGFA**: Nada referiu. **MARINHA**: "…o mais importante será a definição de Doutrina quer ao nível da Cibersegurança e da Ciberdefesa e fundamentalmente na relação entre estas duas áreas essenciais. Também a criação de um quadro técnico de Ciberdefesa nas Forças Armadas, desde que devidamente alimentado, iria permitir que rapidamente as estruturas de Ciberdefesa atingissem a sua FOC o que iria permitir igualmente uma melhor articulação com as entidades da Cibersegurança…" **EXÉRCITO**: Nada referiu. **FORÇA AÉREA**: "…A cooperação entre a ciberdefesa das Forças Armadas e a ciberdefesa da NATO…"

Apêndice D – Entrevistas no CNCS

Tabela n.º Apd D-1 – Análise de entrevistas no CNCS

INDICADOR	Coordenador do CNCS (Prof. Pedro Veiga)
COOPERAÇÃO	**1. Que tipo de ações de coordenação operacional e de autoridade nacional em matéria de cibersegurança tem o CNCS exercido junto das entidades públicas e infraestruturas críticas?** "Os exemplos são diversos, mas podemos citar as atividades periódicas de coordenação, os exercícios também periódicos, bem como a preparação e concretização de operações coordenadas em momentros específicos em que o ciberespaço é um dos domínios de ação." **2. Atendendo às responsabilidades atribuídas ao CCD no quadro legal e à natureza privada dos prestadores de serviços digitais, considera ser possível o CCD assegurar a "liberdade de ação do país no ciberespaço"? Se sim, que articulação e cooperação deverá existir entre o CCD, o CNCS e os demais atores da cibersegurança?** "A pergunta que faz é um dos desafios que tem de ser respondido a curto prazo,…, Está previsto a sua revisão até maio de 2018 data limite também para a transposição da Diretiva NIS. Na próxima semana estarei presente numa reunião em Bruxelas na qual se irá lançar a revisão da Estratégia Europeia de Cibersegurança e é natural que também venha a ter algum impacto na ENSC. No entanto, considero que o CCD deve possuir instrumentos necessários para garantir a liberdade de ação do ciberespaço e em situações específicas como, por exemplo, o estado de sítio. Nestas situações faz todo o sentido que seja o CCD a liderar o processo e naturalmente os prestadores de serviços essenciais serão obrigados a colaborar. No ciberespaço a colaboração, designadamente a troca eficiente de informação, é um dos fatores cruciais para garantir que se protegem os recursos da sociedade digital." **3. De que forma o CCD pode melhorar o seu contributo para a cibersegurança nacional?** "Com uma partilha mais eficaz e mais forte de competências e de conhecimentos nesta área. O CCD tem um conjunto de competências bastante valiosas e deve dar um contributo na capacitação juntamente com o CNCS, mas não na parte operacional. Na parte operacional não deve intervir em situação normal. O CCD pode também apoiar com a coordenação de exercícios de cibersegurança nacionais, de âmbito civil, nos quais se partilhem experiências e se exercite a coordenação numa resposta a ataques. Com a transposição da Diretica SRI os atores militares (CCD) só deverão ser chamados a intervir nas Infraestruturas Criticas e Serviços Essenciais civis em estados de emergência, sitio ou guerra ou em casos que o governo entenda que deva intervir no apoio ao CNCS. A Defesa, nos termos da Constituição, deve-se preparar para eventualmente fazer ataques em casos de conflito, algo que o CNCS não tem mandato e não está preparado."
PARTILHA	**4. De que forma a cibersegurança ganha com a celebração de protocolos/memorandos/acordos com outras entidades públicas ou privadas, nacionais ou internacionais?** "Ganha porque o protocolo, para além de um reforço no relacionamento entre CNCS-Empresa de Serviço Essencial, permite também a troca de um conjunto de informação técnica e operacional, quer sobre as gamas de IP das suas infraestruturas de informação quer dos pontos de contacto de confiança na comunicação mútua. Com a transposição da Diretiva NIS o protocolo deixará de ser tão importante, uma vez que, muito provavelmente, a lei definirá o caráter obrigatório para notificação dessa informação, assim como para o relato de incidentes relevantes para a cibersegurança. É isso que Portugal, pelo menos para já, está a pensar fazer à semelhança de outros países." **5. Tem havido partilha de informação e conhecimento situacional na rede CSIRT que promova um ambiente de cooperação e assistência mútua no tratamento de ciberincidentes? Quais os principais desafios?** "A resposta é muito simples, é sim! Tem havido partilha… E a própria Diretiva NIS prevê o reforço dessa partilha e isso está a ser feito. Tem havido reuniões periódicas ao nível internacional, a última foi no passado mês de fevereiro em Malta. A nível nacional tem havido reuniões com entidades relevantes do Ciberespaço, nomeadamente com o CCD, com a Polícia Judiciária e com os Serviços de Informação. Já a cooperação e articulação dentro da rede CSIRT nacional inclusive com os CSIRT de entidades privadas tem existido mas é algo que ainda tem de ser melhorado. É essencial trazer mais entidades para estas malhas de cooperação. Temos um protocolo com a EDP e em andamento, temos também outros protocolos com o Centro de Ciberdefesa, a REN e a GALP. Desafios!... Trabalhar com a escassez de recursos humanos do CNCS e os ciclos de tomada de decisão extremamente longos, mesmo das empresas, para fazer aprovar os protocolos. Para sermos CSIRT nacional temos de ter as gamas de IP e precisamos da identificação de um ponto de contacto lá e outro cá. Os conceitos e as boas intensões demoram a passar à prática e carecem de medidas mais ativas."

MATURIDADE	**6. Está previsto o CNCS vir a atingir a *Full Operational Capability* num futuro próximo? Existem limitações que possam comprometer prazos ou qualidade no serviço prestado pelo CNCS?** "O CNCS faz três anos no próximo dia 7 de outubro de 2017, e ainda não atingiu a FOC por problemas organizativos diversos que, aliados a restrições orçamentais e demora de aprovação de projetos tem contribuído para dificuldades em concretização dos projetos na sua plenitude . Com a alteração da coordenação do CNCS temos procurado suprir as lacunas que foram identificadas na concretização da ENSC, mas a escassez de meios humanos tem representado um desafio complexo. É uma área em que há uma enorme escassez de recursos humanos e onde o setor privado oferece condições que não conseguimos igualar, traduzindo-se isso em dificuldades de retenção de talento."
GOVERNANCE	**7. O atual modelo *governance* do ciberespaço nacional é o que melhor articula as sinergias existentes e serve o interesse nacional, mesmo em situação de crise?** "Ora bem, a ENSC não identifica devidamente o nível de responsabilidade das várias entidades. Refere uma coordenação política-estratégica para a segurança e defesa do ciberespaço na dependência direta do Primeiro-Ministro, mas que na prática ainda não está totalmente concretizada. Em janeiro, o CNCS propôs ao governo a criação de um Conselho Superior de Cibersegurança (CSCS) ao mesmo tempo que também propôs que este Centro fosse identificado como a Autoridade Nacional de Cibersegurança, no âmbito da Diretiva NIS e o CSIRT Nacional. Mas ainda não obtivemos resposta e essa resposta é muito relevante para moldar o futuro da sociedade digital. Ao CSCS deve competir a coordenação político-estratégica para a segurança e defesa do ciberespaço, assim como dar indicações para o CNCS, para o CCD e para a área do Cibercrime que é gerida pela Polícia Judiciária. Propusemos que na sua composição estejam representados os Ministérios mais relevantes, mas naturalmente o Governo irá decidir e poderá, por exemplo, decidir uma participação mais alargada a todos os Ministérios ou a outras entidades." **8. Uma das competências do CNCS referidas no DL nº 69/2014 de 9 de maio consiste em "assegurar o planeamento da utilização do ciberespaço em situação de crise e de guerra no âmbito do planeamento civil de emergência". Em situação de guerra não deveria ser o CCD a ter essa competência?** "Obviamente, o CNCS não tem essa capacidade, pelo menos com os recursos atuais. Em situação de guerra quem deveria tomar o controlo seria o CCD. Na minha perspetiva é mais uma das ambiguidades que o CSCS, se já estivesse criado, deveria esclarecer. O CNCS tem Know How nalgumas áreas, mas não em todas, e nem constitucionalmente tem mandato, mas sim as Forças Armadas." **9. Os operadores de serviços essenciais referidos no Anexo II (energia, os transportes, a saúde e a banca) abrangem todas as infraestruturas críticas nacionais?** "Bem essa é uma questão que deve ser revisitada porque quem tem a supervisão sobre as Entidades e as Infraestruturas Criticas é a Autoridade Nacional de Proteção Civil, que não está devidamente capacitada para tratar dos problemas do ciberespaço e também ainda não tem uma articulação suficientemente forte com o CNCS. A rápida evolução tecnológica que se tem verificado com a proliferação de TI em todos esses sectores não tem sido acompanhada por idêntica eficiência na colaboração destas entidades e é uma área onde cremos que é importante o estreitamento da colaboração. Penso que a transposição da Diretiva NIS ajudará a esclarecer esta questão."

Departamento Jurídico (MAJ Leite)

PARTILHA	**1. A Diretiva NIS "estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais". Estes requisitos são de caráter obrigatório? Se sim, como e quem poderá verificar e controlar a sua correta implementação?** "Sim. Os artigos 14.º e 16.º da Diretiva NIS estabelecem essa obrigatoriedade. A verificação do cumprimento das obrigações legais que serão criadas será efetuada dando poderes de fiscalização e de auditoria às entidades com responsabilidades no modelo de governance que será implementado. Com a ressalva de ser preconizada uma "light touch approach" para os prestadores de serviços digitais pelo que estes irão identificar os requisitos de segurança e serão objeto de uma supervisão com caráter "ex post" além de outras especificidades de regime. Neste âmbito, o modelo a implementar irá, previsivelmente, assentar numa autoridade nacional competente neste âmbito (o CNCS) e nas entidades reguladoras dos setores previstos na Diretiva NIS." **2. Deverão os operadores identificados, constituir as suas CSIRTs? Se sim, o CNCS tem capacidade para prestar apoio necessário (consultoria, ações de formação, coordenação de exercícios nacionais** **"**A constituição de uma CSIRT não é obrigatória pela Diretiva NIS. O CNCS já o faz no âmbito da sua missão e competências."

COOPERAÇÃO	**3. Tendo em conta que Diretiva NIS visa aumentar a cooperação entre Estados-Membros e desenvolver uma cultura de segurança em sectores críticos, está previsto na transposição reforçar o emprego dual das FFAA no âmbito da cibersegurança nacional?** "A Diretiva NIS não impõe obrigações em matéria de defesa nacional. Acresce que o emprego das Forças Armadas constitui uma prerrogativa exclusivamente nacional. Deste modo, não está prevista qualquer alteração ao âmbito de atuação das Forças Armadas que está preconizado na legislação aplicável."
	4. Para além do CNCS, existem outros organismos representados na equipa jurídica que tem a incumbência de transpor a Diretiva NIS para a ordem jurídica nacional? "A responsabilidade pela coordenação do processo de transposição da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva NIS) foi atribuída à Presidência de Conselho de Ministros e ao Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança (GNS/CNCS). Os trabalhos decorrentes do processo de transposição da Diretiva NIS não são de natureza exclusivamente jurídica. Os trabalhos decorrentes do processo de transposição da Diretiva NIS têm sido desenvolvidos pelo GNS/CNCS em contacto permanente com o Gabinete da Ministra da Presidência e da Modernização Administrativa. O GNS/CNCS tem como premissa para os trabalhos acima referidos integrar os contributos de todas as entidades com responsabilidades no âmbito da Diretiva NIS." **5. Qual é o ponto de situação relativo ao processo de transposição?** "O GNS/CNCS procedeu a uma identificação das entidades que poderão ser identificadas como operadores de serviços essenciais e a uma listagem das entidades que poderão ser enquadradas no conceito de prestadores de serviços digitais. Paralelamente o GNS/CNCS está a elaborar o projeto de ato jurídico que irá transpor para o ordenamento jurídico nacional a Diretiva NIS e a proceder à recolha de contributos de outras entidades neste âmbito. O GNS/CNCS está também a analisar os requisitos constantes da Diretiva NIS relativamente à adoção pelos Estados-Membros de uma Estratégia nacional de segurança das redes e dos sistemas de informação de forma a colaborar na revisão da Estratégia Nacional de Segurança do Ciberespaço." **6. Esta transposição terá em consideração alguma das matérias da Estratégia Nacional de Segurança da Informação ou da Estratégia Nacional de Ciberdefesa em elaboração?** "Nos trabalhos decorrentes do processo de transposição da Diretiva NIS o GNS/CNCS irá ter em consideração todos os referenciais necessários." **7. A quem compete a elaboração e revisão periódica da lista dos operadores de serviços essenciais?** "A identificação em lista e a posterior revisão da identificação dos operadores de serviços essenciais será efetuada pelos Estados-Membros. De forma a assegurar uma abordagem coerente a nível europeu do processo de identificação o Grupo de Cooperação irá auxiliar na realização desta tarefa. A Comissão Europeia irá posteriormente avaliar a identificação e revisão efetuadas." **8. Os operadores de serviços essenciais referidos no Anexo II (energia, os transportes, a saúde e a banca) abrangem todas as infraestruturas críticas nacionais? Serão considerados apenas os nacionais ou todos os que estejam estabelecidos no território nacional?** "O conceito de operador de serviços essenciais não se confunde com o de infraestrutra crítica. Serão considerados os que estejam sujeitos à jurisdição nacional." **9. Para quando (trimestre, semestre/ano) prevê o terminus do processo?** "O prazo de transposição termina em 09 de maio de 2018. No segundo semestre de 2017 será apresentado superiormente um esboço de proposta de lei que posteriormente será objeto de consulta pública e mais tarde seguirá para a Assembleia da República para votação seguindo os demais trâmites legislativos necessários."

Apêndice E – Entrevista na DPED

Tabela n.º Apd E-1 – Entrevista na DPED

INDICADOR	Assessor da Direção de Planeamento Estratégico de Defesa (TCOR Jorge Ralo)
GOVERNANCE	**1. Partindo do princípio que uma intervenção simultânea do CNCS, no âmbito da cibersegurança, e do CCD, no âmbito de ciberdefesa, é autorizada, faria sentido existir uma Estrutura de Governação e Gestão Integrada?** "No caso de uma intervenção simultânea, a Estrutura de Governação e Gestão Integrada entre o CNCS e CCD não só faz todo o sentido como não se afigura ser de outra maneira. No entanto, a legislação para o efeito é nula ou escassa, e a colaboração CNCS/CCD não parece fácil por se encontrarem na dependência de organismos distintos. O CNCS está sob a alçada do Gabinete Nacional de Segurança que depende da Presidência do Conselho de Ministros,…, A ciberdefesa nacional ocupa-se da defesa das infraestruturas críticas nacionais cujo mau funcionamento pode afetar a soberania nacional, atuando dentro e fora do ciberespaço nacional, interagindo com a cibersegurança nacional e com a cibersegurança global,…, O Estado Português tem como tarefa fundamental garantir a independência nacional e criar as condições económicas, sociais e culturais que a promovam. É para o cumprimento desta tarefa que concorre a missão da Defesa Nacional, a par de todos os setores do Estado, contra qualquer agressão ou ameaça externa. A Política de Defesa Nacional integra os Princípios, os Objetivos, as Orientações e as Prioridades definidos na Constituição, na Lei de Defesa Nacional, no Programa do Governo e no Conceito Estratégico de Defesa Nacional (CEDN) respetivamente. E inclui ainda as políticas sectoriais do Estado necessárias para o cumprimento dos objetivos da Defesa Nacional, consagradas na Lei Defesa 2020 e na Orientação Política para a Ciberdefesa. A globalização veio difundir as ameaças e os riscos em todas as dimensões, onde se incluem os ataques cibernéticos e todo o seu potencial devastador. Neste contexto de combate às ameaças no ciberespaço, a Lei de Defesa Nacional atribui ao Ministro da Defesa Nacional a responsabilidade de garantir a colaboração das Forças Armadas com as forças e serviços de segurança, em particular com o Sistema de Segurança Interna, com o Sistema de Informações da República Portuguesa e com a Comissão Nacional de Proteção Civil,…, Falta definir a Estratégia Nacional de Ciberdefesa que consubstancie um Plano de Ação e contribua para o reforço das capacidades nacionais de cibersegurança e ciberdefesa Posso adiantar-lhe que não sei quando sairá mas tenho a certeza que assentará em 5 pontos fundamentais: - Estrutura de Governação e Gestão Integrada (Aproximação coerente entre a Cibersegurança e a Ciberdefesa) - Investimento no fator humano - Partilha de informação - Investimento em equipamento e infraestruturas adequadas - Cooperação e colaboração Nacional e Internacional