INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR

2019/2020 1ª Edição

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL (TII)

O MODELO DE CIBERDEFESA NACIONAL. SOLUÇÃO CENTRALIZADA OU DISTRIBUÍDA?

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

Pedro Miguel de Castro Pinho

1TEN M-AV

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O MODELO DE CIBERDEFESA NACIONAL. SOLUÇÃO CENTRALIZADA OU DISTRIBUÍDA?

1TEN M-AV Pedro Miguel de Castro Pinho

Trabalho de Investigação Individual do CPOS-M

Pedrouços 2020

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O MODELO DE CIBERDEFESA NACIONAL. SOLUÇÃO CENTRALIZADA OU DISTRIBUÍDA?

1TEN M-AV Pedro Miguel de Castro Pinho

Trabalho de Investigação Individual do CPOS-M

Orientador: Capitão-de-fragata (CFR) M Ricardo Cordeiro de Almeida

Pedrouços 2020

Declaração de compromisso Antiplágio

Eu, **Pedro Miguel de Castro Pinho**, declaro por minha honra que o documento intitulado **"O MODELO DE CIBERDEFESA NACIONAL. SOLUÇÃO CENTRALIZADA OU DISTRIBUÍDA?"** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **CPOS – M 2019/20 1ª Edição** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

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

Pedrouços**, 26** de **janeiro** de **2020**

Pedro Miguel de Castro Pinho

Assinatura

Agradecimentos

Cada Homem deve ter em si um código de conduta para pautar e orientar a sua vida e as suas ações. Posso sem sombra de dúvidas referir que o meu é a minha família. Assim sendo, dedico este trabalho à minha família, especialmente à minha esposa e às minhas filhas que no decorrer de todo este percurso se viram privadas de muitas horas de convivência e de brincadeira. Faltei com algum apoio e suporte que souberam superar com mestria, força de vontade e muita compreensão. Por tudo isso, para elas vai o meu maior agradecimento.

Agradeço ao meu orientador, CFR Cordeiro de Almeida pelo apoio dado, sugerindo caminhos e desconstruindo o meu pensamento de modo a torná-lo mais esclarecido, ajudando-me em todo o percurso.

De igual forma, houve muitas outras pessoas que tiveram uma pronta disponibilidade para colaborarem. O seu contributo foi precioso para levar a bom porto este trabalho, revelando nas entrevistas efetuadas, novas perspetivas que me permitiram ver outras abordagens. Ao Contra-almirante (CALM) Gameiro Marques, ao Capitão-de-mar-e-guerra (CMG) Fialho de Jesus, ao Coronel Quaresma Rosa, ao Tenente-coronel (TCOR) José Teixeira, ao CFR Câmara de Assunção, ao CFR Caldeira de Carvalho, ao Major (MAJ) André Castro e ao Capitão-tenente (CTEN) Courela Alexandre estou profundamente agradecido.

Agradeço ao TCOR Silva Costa pela ajuda providenciada numa fase embrionária do meu trabalho, permitindo-me olhar o mesmo de outra perspetiva e de uma forma mais completa.

Por fim, mas de modo igualmente importante agradeço à primeiro-tenente Rute Branco e ao primeiro-tenente Miguel Pinheiro pelo mútuo incentivo e apoio.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Índice de Tabelas

Resumo

O ano de 2016 marcou de forma indelével o encetar de alterações profundas na forma como os países olhavam para o ciberespaço consubstanciando-se através do reconhecimento deste pela *North Atlantic Treaty Organization* (NATO) como Domínio Operacional (DO) aquando da Cimeira de Varsóvia.

Conjuntamente, em Portugal ocorriam reformas nas estruturas estatais onde palavras como eficiência, concentração de recursos, e integração de capacidades ganharam uma nova vida. Analogamente as Forças Armadas (FFAA) foram incluídas neste processo com a determinação para conglutinar recursos que tenham um campo de aplicação transversal aos ramos.

Mormente na ciberdefesa (CD), foi elaborado e aprovado em 2019 o "*Plano de Desenvolvimento da Capacidade de Ciberdefesa*" que preconiza uma profunda reestruturação do Centro de Ciberdefesa (CCD) apresentando uma nova estrutura, mais robusta, acarretando um aumento de recursos humanos (RH) substancial até ao final de 2021 (EMGFA, 2019b), o que poderá ter implicações nos núcleos *Computer Incident Response Capability* (CIRC) dos ramos.

Neste sentido, surge este trabalho, baseado num raciocínio dedutivo, suportado por pesquisa bibliográfica e pela realização de entrevistas a especialistas na matéria, avaliando, de entre dois modelos de CIRC apresentados, qual o que melhor contribui para a edificação da capacidade de CD, adaptando-se às necessidades das FFAA.

Concluiu-se que o modelo centralizado se apresenta como sendo aquele que, face ao ambiente interno e externo atual, tem mais potencialidade para contribuir positivamente para a edificação da capacidade de CD nas FFAA, alinhando-se com os objetivos do "Plano".

Palavras-chave

Centro de Ciberdefesa, CIRC, Ciberdefesa, Capacidade

Abstract

The year of 2016 was indelibly marked by profound changes in the way as countries looked to cyberspace through its recognition by the North Atlantic Treaty Organization (NATO) *as Operational Domain at the Warsaw Summit*.

At the same time, in Portugal occurred reforms in state structures where words such as efficiency, resource concentration and integrated capabilities achieved new meaning and importance. Similarly, the Armed Forces were included in this process with the determination to combine resources that were common to them.

Particularly in cyber defence, was prepared and approved in 2019 the "Cyber Defence Capability Development Plan" that advocates a deep restructuring in the Cyber Defence Centre, presenting a new structure, more robust which entails a substantial increase of human resources until the end of 2021 (EMGFA, 2019b). *That could have repercussions in the Computer Incident Response Capability (CIRC).*

With that purpose arises this work that was based in a deductive method, supported by bibliographic analyses and interviews made to experts in the subject, and pretends to evaluate, between the two models of CIRC presented, which best contributes to build up the cyber defence capability, adapting to the needs of the Armed Forces.

It has been concluded that the centralized model presents them self as the one which, given the current internal and external cyber environment, has more potential to contribute positively to build up the cyber defence capability in the Armed Forces, aligned with the objectives outlined in the "Cyber Defence Capability Development Plan".

Keywords

Cyber Defence Centre, CIRC, Cyber defence, Capability

Lista de abreviaturas, siglas e acrónimos

AP	Administração Pública
CAIH	*Cyber Academia and Innovation Hub*
CALM	Contra-almirante
CCD	Centro de Ciberdefesa
CCDCOE	*Cooperative Cyber Defence Centre Of Excellence*
CD	Ciberdefesa
CE	Conceito Estratégico
CEDN	Conceito Estratégico de Defesa Nacional
CEM	Conceito Estratégico Militar
CFR	Capitão-de-fragata
CIRC	*Computer Incident Response Capability*
CMG	Capitão-de-mar-e-guerra
CNCS	Centro Nacional de Cibersegurança
CS	Cibersegurança
CSIRT	*Computer Security Incident Response Team*
CTEN	Capitão-tenente
DAM	*Digital Attack Map*
DDoS	*Distributed Denial of Service*
DE	Diretiva Estratégica
DL	Decreto de Lei
DO	Domínio Operacional
DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestrutura, Interoperabilidade
DR	Decreto Regulamentar
EMGFA	Estado-Maior General das Forças Armadas
ENCD	Estratégia Nacional de Ciberdefesa
ENISA	*European Union Agency for Network and Information Security*
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EUA	Estados Unidos da América
FFAA	Forças Armadas
FAP	Força Aérea Portuguesa
GT	Grupo de Trabalho

IE	Infraestruturas
IEFP	Instituto de Emprego e Formação Profissional
IO	Interoperabilidade
IoE	*Internet of Everything*
IoT	*Internet of Things*
LA	Linha de Ação
LO	Lei Orgânica
LPM	Lei de Programação Militar
MAJ	Major
MDN	Ministério da Defesa Nacional
MN CD E&T	*Multinational Cyber Defence Education and Training*
NATO	*North Atlantic Treaty Organization*
NCIA	NATO *Communication and Information Academy*
NIST	*National Institute of Standards and Technology*
OE	Objetivo Específico
OG	Objetivo Geral
PCM	Presidência do Conselho de Ministros
PESTAL	Político, Económico, Sociocultural, Técnico, Ambiente, Legal
PIB	Produto Interno Bruto
QC	Questão Central
QD	Questão Derivada
QO	Quadro Orgânico
RCM	Resolução do Conselho de Ministros
RH	Recursos Humanos
RRT	*Rapid Response Teams*
SOP	*Standing Operating Procedures*
SWOT	*Strengths, Weaknesses, Opportunities, Threats*
TCOR	Tenente-coronel
TIC	Tecnologias da Informação e Comunicações
TTP	Táticas, Técnicas e Procedimentos
UNC3T	Unidade Nacional de Combate ao Cibercrime Tecnológico
UE	União Europeia
WEF	*World Economic Forum*

Introdução

A acentuada evolução tecnológica traduziu-se entre outras, na incrementação de uma economia centrada em rede permitindo o acesso facilitado a consumidores, empresas e mesmo a Estados a serviços digitais globais e ao desenvolvimento de serviços inovadores aprofundando a cultura de partilha e conetividade.

Portugal acompanha a tendência global tendo a economia digital em 2017 um peso de 4,6% do Produto Interno Bruto (PIB) prevendo-se um crescimento até cerca de 10% até 2025 (Ferreira R. R., 2019).

Este crescendo tecnológico, acarreta igualmente ameaças e riscos da mais diversa índole, podendo afetar o regular funcionamento de instituições e ameaçando inclusive a soberania dos Estados, conforme se verificou decorrente de diversos incidentes em vários países (RCM 19/2013, 2013a) (EMGFA, 2019a).

Estas ameaças trouxeram apreensões à NATO, à União Europeia (UE) e aos Estados que desde 2002 têm desenvolvido as suas competências na segurança do ciberespaço a diversos níveis, atingindo um marco importante em 2016, na cimeira de Varsóvia, onde a NATO reconheceu o ciberespaço como quarto (4º) DO, reconhecendo e permitindo operações no e através do ciberespaço (Nunes, et al., 2018).

Em Portugal, nomeadamente no que concerne às FFAA, denota-se essa maior preocupação a partir de 2013, quando foi emanado o Conceito Estratégico de Defesa Nacional (CEDN) através da Resolução do Conselho de Ministros (RCM) nº 19/2013, que aponta a cibercriminalidade como um dos principais "riscos e ameaças à segurança nacional". Esta preocupação trouxe um novo mercado de trabalho que sendo tão especializado e abrangendo tantas empresas e setores da sociedade, não foi possível até ao presente momento suprir as necessidades de RH afetos à segurança do ciberespaço, havendo uma enorme lacuna por preencher (RCM 19/2013, 2013a, p. 1985).

Com a promulgação do Decreto de Lei (DL) nº 184/2014 e consequente Decreto Regulamentar (DR) nº 13/2015 que aprovaram a nova orgânica do Estado-Maior General das Forças Armadas (EMGFA), foi incluído na estrutura do mesmo o CCD, referindo igualmente os CIRC dos ramos das FFAA (DL 184/2014, 2014) (DR 13/2015, 2015).

Os CIRC, "cuja competência é a de resposta a incidentes de segurança da informação através da deteção, identificação, mitigação e resposta ao incidente, nas redes e sistemas de

informação da sua responsabilidade" não têm conseguido atingir a sua *Full Operational Capability* tendo falta de RH alocados aos mesmos (EMGFA, 2019a, p. 11).

De acordo com a Diretiva Estratégica (DE) do EMGFA de 2018 existe a necessidade de "dinamizar a edificação da capacidade[1] de CD nacional" (CEMGFA, 2018, p. 3). Para tal foi criado um grupo de trabalho (GT) como o propósito de "estabelecer um plano estratégico" de modo a atingir o preconizado na DE referida (EMGFA, 2019a, p. 1). Decorrente do mesmo foi elaborado um relatório e apresentado o "*Plano de Desenvolvimento da Capacidade de Ciberdefesa*", doravante referido como "Plano". Esse "Plano" preconiza uma reestruturação do CCD, tornando-se mais robusta, acarretando um aumento de RH até ao final de 2021 (EMGFA, 2019b).

Estando o ambiente cibernético em constante evolução torna-se premente analisar o estado atual do mesmo e referindo-nos especificamente à CD, existem diversos modelos utilizados por nações aliadas com mais experiência nesta área. Sendo um tema atual e mediático e estando já emanado o relatório do GT e a decorrer o "Plano" importa perceber o impacto que este terá nos núcleos CIRC dos ramos e avaliar qual o modelo de CIRC que melhor contribui para a edificação da capacidade de CD, adaptando-se às necessidades das FFAA, face à já mencionada falta de RH especializados na segurança do ciberespaço e às necessidades a breve trecho do CCD.

Este trabalho encontra-se organizado em capítulos sendo primeiramente efetuado um enquadramento conceptual e metodológico e apresentação do modelo de análise. No segundo capítulo far-se-á uma análise do ambiente cibernético, enquanto que no capítulo três ir-se-á comparar os dois modelos averiguando as vantagens e desvantagens em cada um deles. O quarto capítulo visa responder à questão central (QC) avaliando qual o melhor modelo para o objetivo em questão, seguindo-se as conclusões resumindo os resultados, realçando os contributos da investigação e identificando possíveis investigações futuras.

[1] *Vide* Anexo A.

1. Enquadramento

Ao longo deste capítulo ir-se-á enquadrar este estudo a nível dos conceitos de cibersegurança (CS), CD e ciberespaço. Far-se-á também um enquadramento metodológico bem como a explicação do modelo de análise utilizado.

1.1. Enquadramento conceptual

O ciberespaço tendo sido reconhecido em 2016 pela NATO como o 4º DO[2] (NATO, 2017), sendo o único que foi criado pelo Homem (Ferreira L. M., 2018) e que é transversal aos outros quatro DO (Figura 1). Este DO apresenta-se como um "ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas e redes e sistemas de informação" (Figura 2). Perspetiva "novas possibilidades e oportunidades" bem como "ameaça e risco com a ocorrência de incidentes que podem trazer impactos económicos e sociais que não podem ser negligenciados" (RCM 92/2019, 2019, p. 2889) (CNCS, 2019b, p. 12).

Figura 1 – Domínios Operacionais

Fonte: (Neves, 2015)

[2] A NATO considerou o espaço exterior como DO em 2019 sendo que alguns países já o consideram há mais tempo (NATO, 2019).

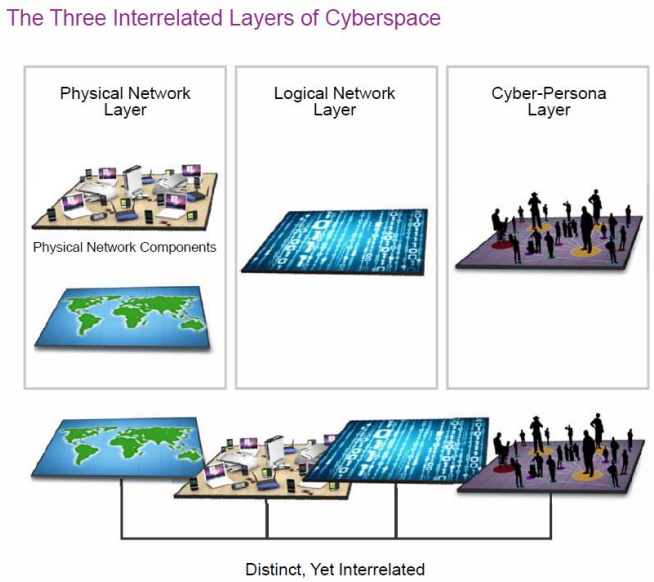

Figura 2 – Camadas do ciberespaço[3]

Fonte: (US, 2018, pp. I-3)

A CS, encontra-se definida como sendo o "conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" estando as suas operações divididas conforme a Figura 3 (RCM 92/2019, 2019, p. 2889).

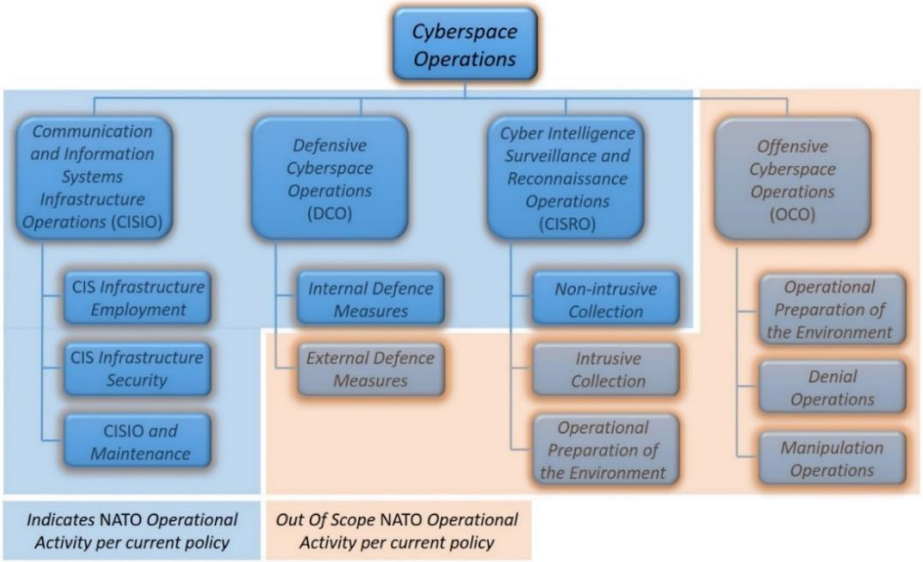

Figura 3 – Operações Ciberespaço[4]

Fonte: Adaptado de (NATO, 2018, pp. A-1-1)

[3] Representação aceite pela NATO e pela maioria dos países, existindo outras.
[4] Existem outras categorizações sendo esta a mais recente.

A CS nacional contribui para garantir a utilização segura do ciberespaço aos seus utilizadores bem como a salvaguarda da Segurança e Defesa Nacional, uma vez que o ciberespaço é uma área de responsabilidade que obedece às mesmas lógicas, competências e ameaças que caracterizam a Segurança e Defesa do Estado sendo essa garantia essencial para a manutenção da segurança e da sobrevivência do país (Nunes P. F., 2012).

Conforme ilustrado na Figura 4, não podemos dissociar a CS da CD pois a segunda é parte integrante da primeira com as devidas diferenças elencadas. "A proteção, deteção e reação têm a ver essencialmente com a área da CS ao passo que o deter e o defender se encontram mais ligadas à CD"[5] (Nunes P. F., 2012, p. 122) (RCM 92/2019, 2019).

Figura 4 – Cibersegurança Nacional (um edifício, vários pilares)

Fonte: (Nunes P. F., 2012)

1.2. Modelo de Análise

O modelo de análise utilizado (Quadro 1), visa responder aos Objetivos Específicos (OE) que decorrem do Objetivo Geral (OG), conforme versados no Modelo de Análise, bem como responder à QC e às Questões Derivadas (QD).

Face à abrangência do tema proposto, houve a necessidade de limitar o mesmo quanto às três dimensões, conteúdo, temporal e espacial (Santos, et al., 2019).

Quanto ao conteúdo, delimitou-se o tema apenas a dois modelos CIRC, um modelo descentralizado, que é o que atualmente se encontra em vigor, e um modelo centralizado onde exista apenas um CIRC comum, modelos esses que serão retratados especificamente

[5] *Vide* Anexo A.

no capítulo 3. A nível espacial, delimitou-se o tema ao CCD e aos CIRC dos ramos e a nível temporal, desde 2013, pois foi nesse ano que foi emanado o CEDN, até à atualidade.

Quadro 1 - Modelo de Análise

Objetivos	Questões	Dimensões	Indicadores
OE 1 Descrever o atual ambiente cibernético	**QD 1** Como se caracteriza o atual ambiente cibernético?	Externo	**P**olítico
			Económico
			Sociocultural
			Tecnológico
			Ambiental
			Legal
		Interno	Perspetiva Genética
			Perspetiva Estrutural
			Perspetiva Operacional
OE 2 Comparar os dois modelos preconizados	**QD 2** Quais as vantagens e desvantagens dos modelos apresentados?	Capacidade	**D**outrina
			Organização
			Treino
			Material
			Liderança
			Pessoal
			Infraestruturas
			Interoperabilidade
OG Avaliar qual o modelo de CIRC que melhor contribui para a edificação da capacidade de CD, adaptando-se às necessidades das FFAA	**QC** Qual o modelo de CD, no âmbito dos CIRC, que melhor contribui para a edificação da capacidade de CD?	Eficácia[6] Eficiência[7]	***S**trengths* (Pontos Fortes)
			***W**eaknesses* (Pontos Fracos)
			***O**pportunities* (Oportunidades)
			***T**hreats* (Ameaças)

1.3. Enquadramento metodológico

Utilizou-se uma filosofia ontológica construtivista pois considerou-se que os fenómenos sociais e os seus significados são produzidos pela interação social e estão em

[6] *Vide* Anexo A.
[7] Idem.

constante reconstrução (Santos, et al., 2019), denotado pela alteração da realidade do ciberespaço, fruto da alteração de comportamentos e de utilização do mesmo, aliada a uma epistemologia interpretativista, na qual "compete ao investigador não só verificar os fenómenos, mas também compreender os significados subjetivos desses mesmos fenómenos sociais" (Santos, et al., 2019, p. 18), isto devido ao facto de, nas conclusões retiradas, se terem interpretado documentos e utilizado a opinião de especialistas na área.

Usou-se o raciocínio dedutivo uma vez que se partiu do geral para o particular, não se tratando da verdade dos factos, mas sim da sua validade, conjugado com o pensamento crítico (Santos, et al., 2019).

Empregou-se uma estratégia de investigação mista uma vez que se efetuou um reforço da estratégica qualitativa, onde se procura "alcançar um entendimento mais profundo e subjetivo do objeto de estudo", através da utilização da apresentação numérica de resultados (Santos, et al., 2019).

Como técnicas de recolha, recorreu-se à análise documental e a entrevistas semiestruturadas a especialistas na área. A "vantagem deste método" (entrevista) "reside na melhoria da comparatividade e da estruturação dos dados, pelo uso coerente do guião da entrevista" bem como a obtenção e complementaridade de dados não possíveis de obter a partir da análise documental (Santos, et al., 2019).

O trabalho decorreu em três fases, a exploratória, a analítica e a conclusiva.

Na fase exploratória efetuou-se a definição inicial do "Estado da Arte" através de revisão de literatura e de entrevistas exploratórias (Santos, et al., 2019), nomeadamente no que concerne ao enquadramento de atuação dos CIRC e no que realmente eles conseguem garantir.

Na segunda fase efetuou-se recolha de informação em diversas fontes de modo a conseguir atingir o OE1.

Para atingir o OE2 recorreu-se simultaneamente a entrevistas a especialistas e recolha de informação, através de análise documental. Não se definiu inicialmente uma quantidade inicial de entrevistas a efetuar, sendo identificadas as unidades importantes para a recolha de informação, tendo-se alcançado saturação de resultados, face às respostas similares obtidas nas entrevistas efetuadas (Rego, Cunha, & Meyer, 2018).

A fase conclusiva visa na sua essência, responder às QD, conjugando esses corolários de modo a responder à QC, atingindo o OG, utilizando-se diversas análises, consoante o adequado a cada dimensão estudada (Figura 5).

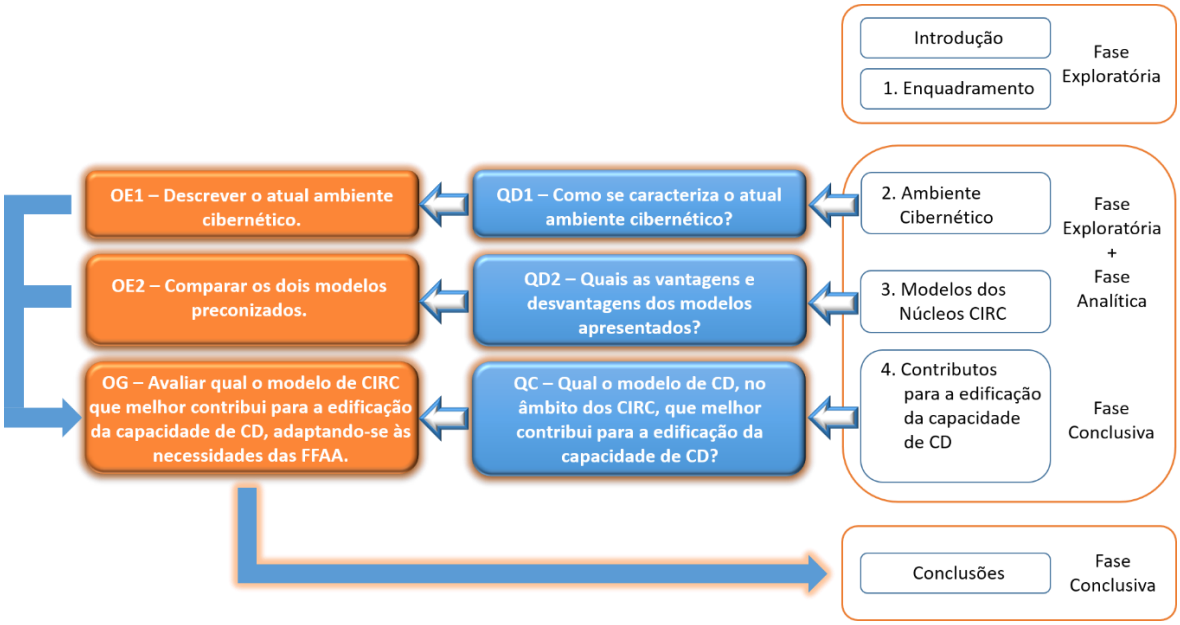

Figura 5 – Percurso Metodológico

2. Ambiente cibernético

Neste capítulo, pretende-se responder à QD1, atingindo o OE1, descrevendo o ambiente cibernético, externo e interno.

2.1. Ambiente externo[8]

Efetuou-se a análise ao ambiente externo utilizando a análise PESTAL[9] apresentando-se de seguida um resumo de cada uma das vertentes, remetendo-se para o Apêndice A uma análise alargada.

2.1.1. Fator Político

Foram elaborados diversos documentos e iniciativas no seio da NATO (Figura 6) e da UE (Figura 7) com o propósito de enquadrar a atuação no ciberespaço fruto da crescente importância do mesmo nos últimos anos.

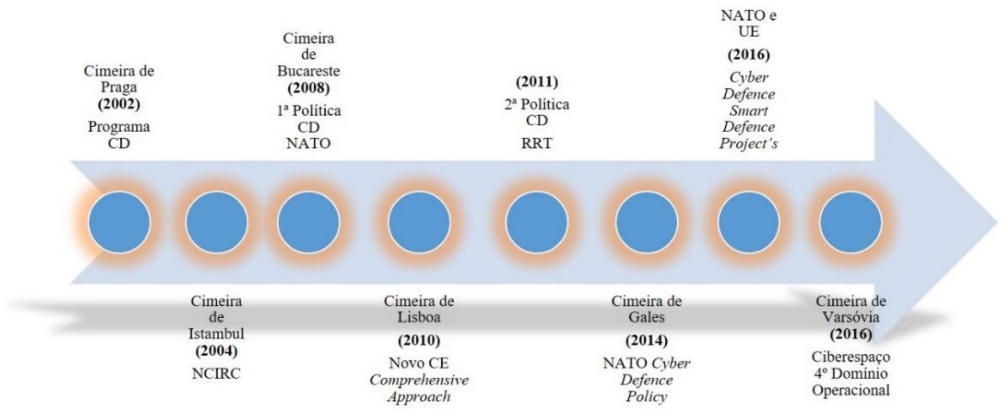

Figura 6 – Cronologia NATO

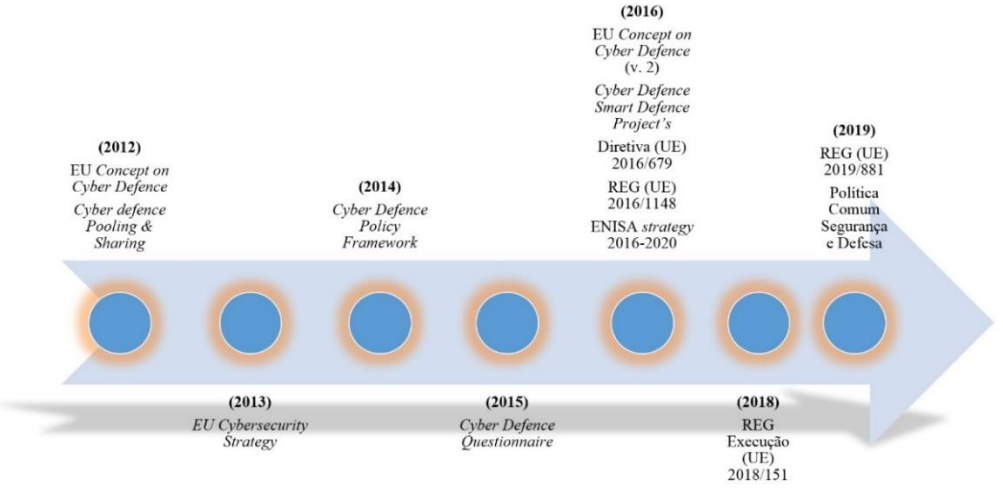

Figura 7 – Cronologia UE

[8] Considerou-se ambiente externo o ambiente fora das FFAA.
[9] Análise que visa o meio envolvente geral. PESTAL - Político, Económico, Sociocultural, Técnico, Ambiental, Legal, do inglês *Political, Economical, Social, Technological, Environmental and Legal. Vide* Anexo A.

Também a nível nacional se tem dado uma cada vez maior importância a este DO tendo sido emanadas diversas iniciativas políticas, direta ou indiretamente relacionadas com CS (CNCS, 2019b) e CD (Figura 8). Alguns destes diplomas encontram-se intrinsecamente relacionados com as FFAA que se irão abordar igualmente noutras vertentes da análise PESTAL, bem como na análise do ambiente interno.

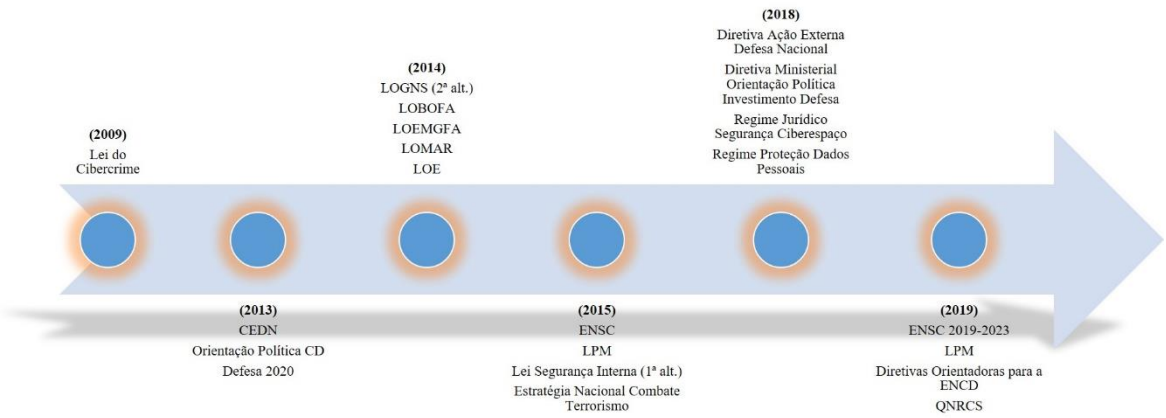

Figura 8 – Cronologia Portugal

2.1.2. Fator Económico

A denominada "Era da Informação" "caracterizada pela existência de uma economia cada vez mais centrada em rede" convida a ações maliciosas no ciberespaço tendo por alvo "indivíduos, organizações ou até Estados, afetando os processos de geração de riqueza" (Nunes, et al., 2018, p. 13).

Tem-se assistido na UE a uma diminuição dos gastos com a defesa enquanto "outros intervenientes globais" reforçam o referido setor, denotando-se também muitos gastos na UE devido à falta de cooperação (Comissão, Europeia, 2016, p. 3).

Também em Portugal se assistiu, nomeadamente através da Lei de Programação Militar (LPM), promulgada através de Lei Orgânica (LO), a um incremento orçamental na CD, podendo ser justificado pelo crescente peso da economia digital, prevendo-se igualmente um aumento das perdas decorrentes de ataques cibernéticos (LO 7/2015, 2015) (LO 2/2019, 2019) (Ferreira R. R., 2019) (Pinto, 2019).

2.1.3. Fator Sociocultural

Com a "Era da Informação" é notório o aumento de utilizadores da Internet (Figura 9), que sendo positivo, acarreta o equivalente negativismo denotado pelo aumento do número

de ciberataques ao longo dos anos, traduzindo-se numa preocupação global com os ciberataques e com o acesso a infraestruturas (IE) críticas (Figuras 10 e 11).

Figura 9 – *Digital, Social & Mobile* (2015, 2019)

Fonte: (wearesocial, 2015) (wearesocial, 2019)

Figura 10 – Riscos Globais (2015)

Fonte: (WEF, 2016)

Figura 11 – Riscos Globais (2019)

Fonte: (WEF, 2019)

Começa-se a verificar a utilização do ciberespaço para projeção de "redes terroristas e de crime organizado" (RCM 19/2013, 2013a, p. 1983) "agilizando a criação de movimentos, a partilha de ideologias e mesmo potenciando revoluções" (Nunes, et al., 2018, p. 20).

A denominada geração dos *millennials*, onde é dada menor relevância a um "emprego para a vida", apresenta como consequência a problemática da retenção de RH podendo estar a reverter-se essa tendência com a chegada ao mercado de trabalho da "geração Z" (Mateus, 2019).

2.1.4. Fator Tecnológico

A acentuada evolução tecnológica evidenciou o facto de o ciberespaço não ser "limitado pela esfera pública ou privada, civil ou militar, interna ou externa" (Nunes, et al., 2018, p. 11) começando-se a falar primeiramente da denominada *Internet of Things*[10] (IoT) que "*scales up to include smart cities*" (Kobie, 2015).

Evoluiu também a definição passando a denominar-se *Internet of Everything*[11] (IoE) que é a ligação de "pessoas, processos, dados e coisas" assumindo-se que o pilar "coisas" corresponde à IoT (Santos L. , 2016).

[10] *Vide* Anexo A.
[11] Idem.

De modo a educar ciberneticamente os cidadãos, procurando diminuir o seu próprio risco, face ao crescente número de ciberataques, conforme exemplo dado nas Figuras 12 a 16, o Centro Nacional de Cibersegurança (CNCS) tem o curso "Cidadão Ciberseguro". Colabora com os restantes *players* da CS nacional (Figura 17) e é interoperável com a rede *Computer Security Incident Response Team*[12] (CSIRT) (Figura 18) (CNCS, 2019a).

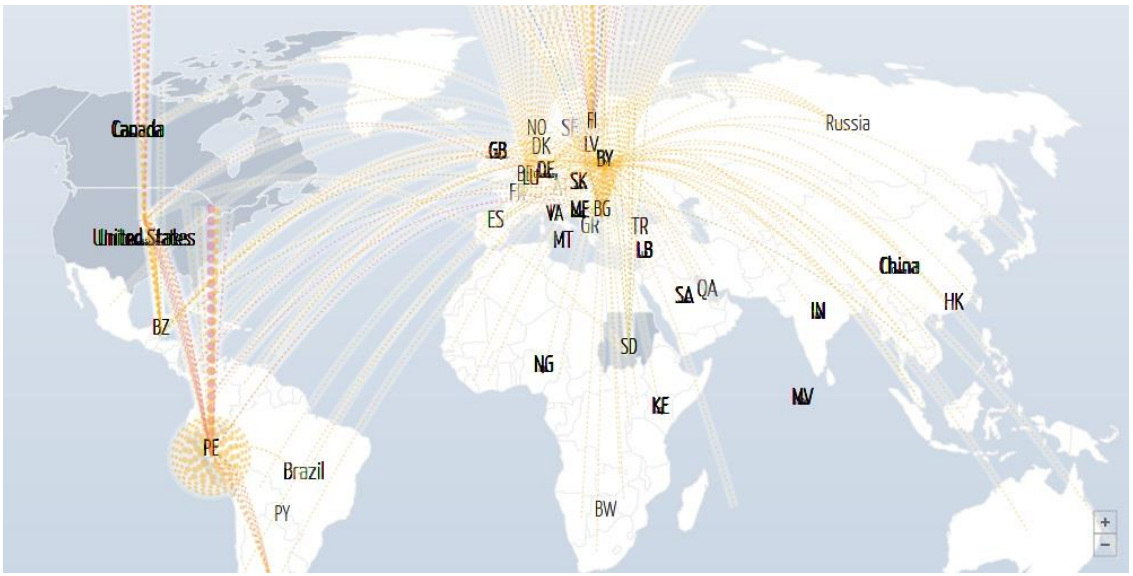

Figura 12 – Ataques DDoS mundiais (02/01/2015)

Fonte: (Ideas & Networks, 2015)

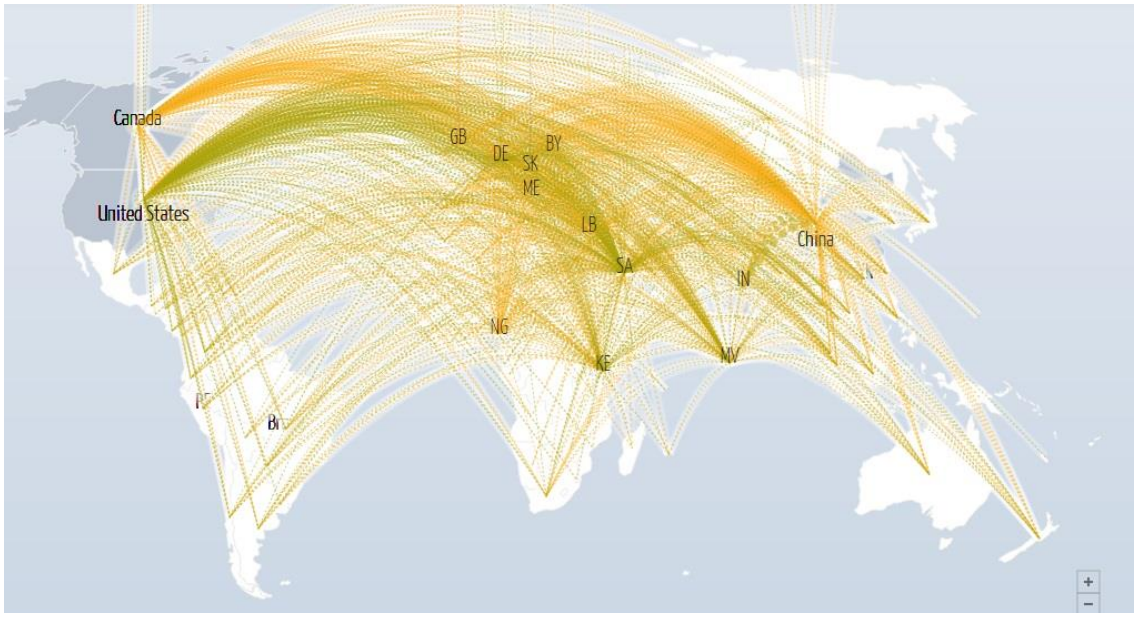

Figura 13 – Ataques DDoS mundiais (12/11/2019)

Fonte: (Ideas & Networks, 2019)

[12] *Vide* Anexo A.

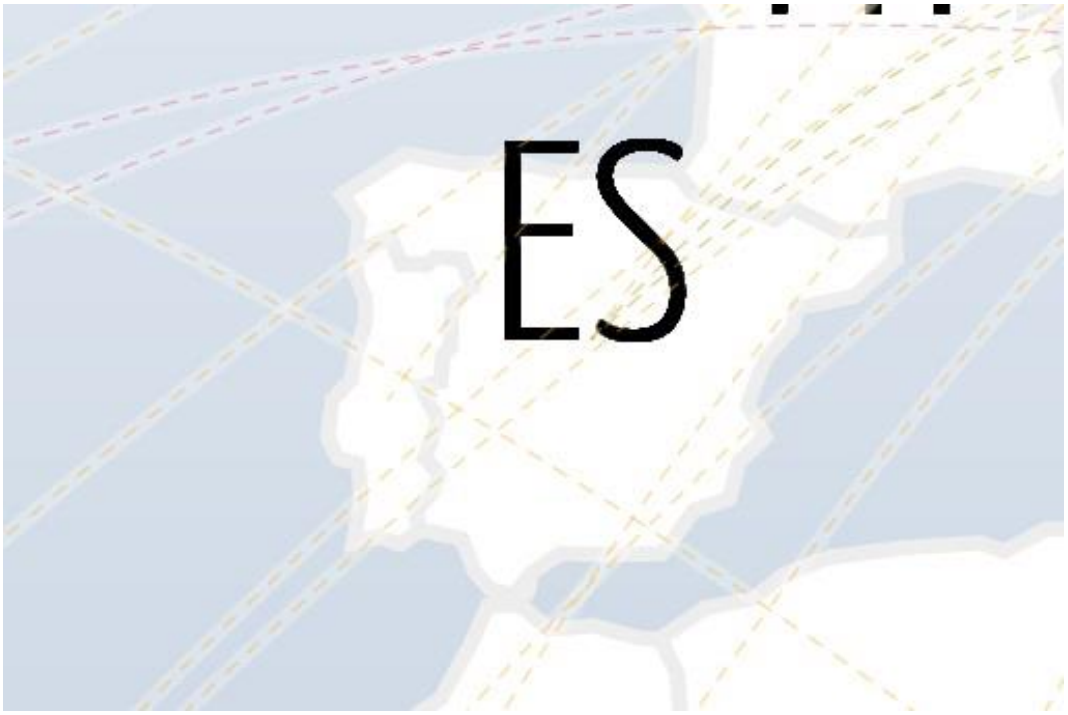

Figura 14 – Ataques DDoS Portugal (02/01/2015)

Fonte: (Ideas & Networks, 2015)

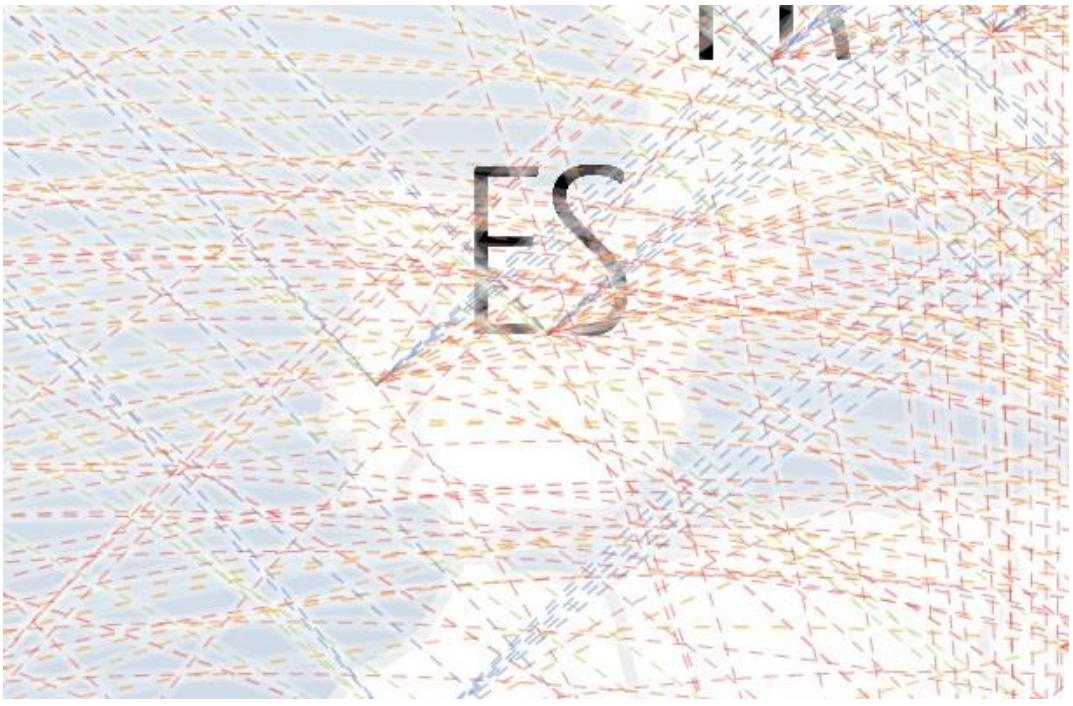

Figura 15 – Ataques DDoS Portugal (12/11/2019)

Fonte: (Ideas & Networks, 2019)

Figura 16 – Ataques DDoS (2015-2019)

Fonte: (Ideas & Networks, 2019)

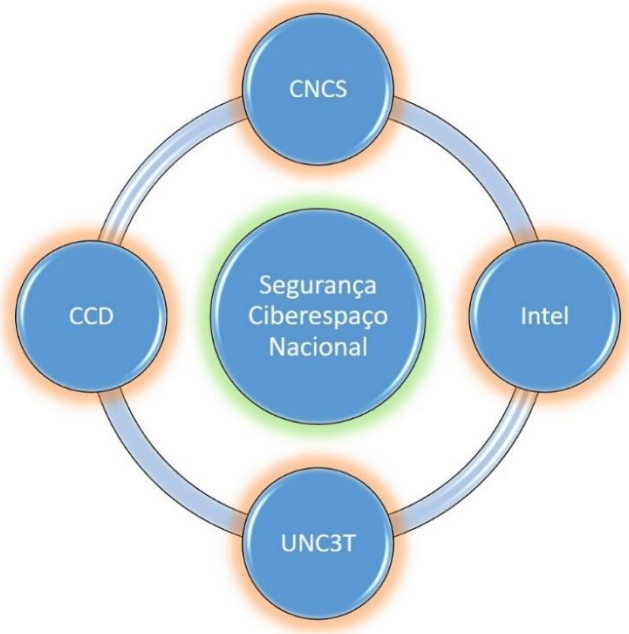

Figura 17 – *Players* Segurança Ciberespaço Nacional

Fonte: Adaptado de (Marques, 2019)

Figura 18 – Rede CSIRT nacional

Fonte: (RNCSIRT, 2019)

2.1.5. Fator Ambiental[13]

O "ambiente mundial se tornou mais incerto e menos seguro" (Regulamento (UE) 2019/881, 2019, p. L 151/18) tendo o ambiente cibernético características próprias como "caráter dinâmico", "baixo custo de acesso", "enorme potencial de crescimento", "alta capacidade de processamento de informação", "caráter assimétrico", "anonimato", "alta capacidade para produzir efeitos físicos", "transversalidade dos seus impactos" (Bernardino, 2015, p. 17) favorecendo ataques ao normal funcionamento dos Estados sendo o combate às ameaças assente no princípio da indivisibilidade da segurança (Nunes, et al., 2018).

Existem IE e serviços nacionais que pela sua relevância têm grande impacto económico-financeiro, intitulados de IE críticas e serviços essenciais respetivamente, conforme Figuras 19 e 20.

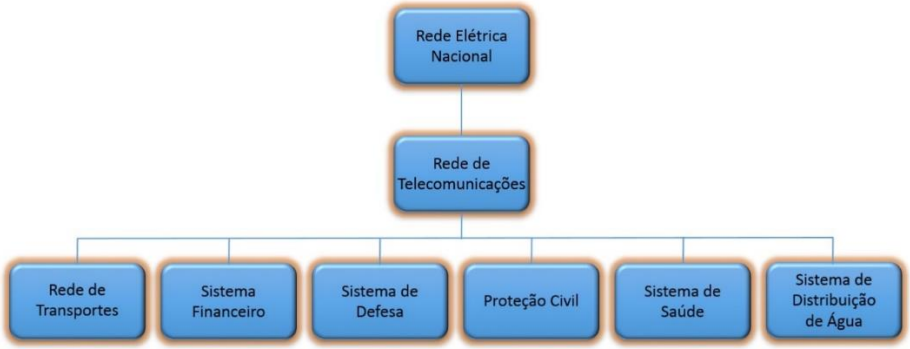

Figura 19 – Interdependência das IE Críticas Nacionais

Fonte: Adaptado de: (Aparício, 2017)

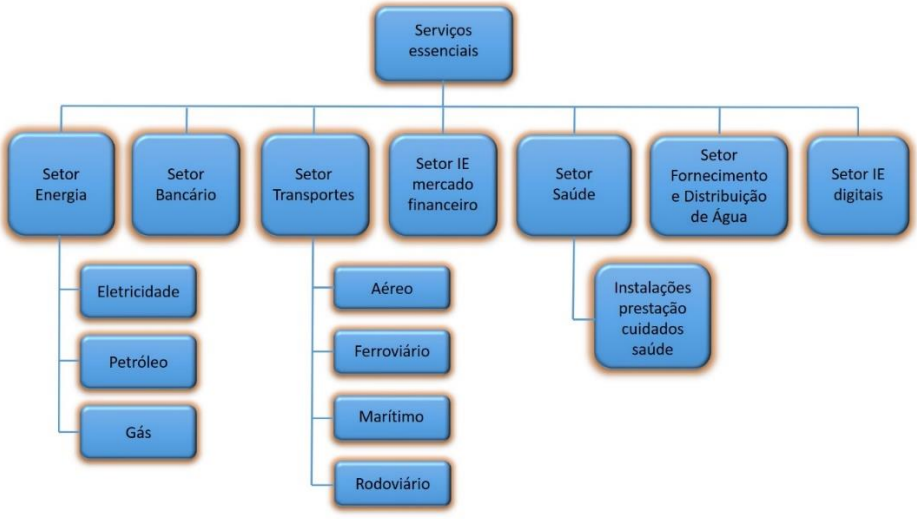

Figura 20 –Serviços Essenciais Nacionais

Fonte: Adaptado de: (L 46/2018, 2018, p. 4037)

[13] Considera-se o ambiente cibernético e não as questões ambientais.

2.1.6. Fator Legal

Sendo o ciberespaço caracterizado por ser um "espaço aberto desprovido de fronteiras tangíveis," é imprescindível promover a cooperação entre Estados e no seio de organizações internacionais (DESPACHO 13692/2013, 2013, p. 31977).

A NATO tomou algumas posições importantes reconhecendo a "aplicabilidade do Direito Internacional" podendo um ciberataque ser considerado "de acordo com a Carta das Nações Unidas (Artigo 51º)" e invocar o "Artigo 5º do Tratado de Washington". O *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) promulgou o Manual de Tallinn "apontando respostas para questões jurídicas" (Nunes, et al., 2018, p. 40 e 51).

A UE tomou diversas iniciativas, principalmente relacionadas com a segurança, nomeadamente sobre "tratamento de dados pessoais" (Regulamento (UE) 2016/679, 2016a, p. L 119/1).

Em Portugal foi emanada diversa legislação respeitante ao ciberespaço, mas apesar disso num "Estado de Direito, a segurança e a defesa têm de atuar num quadro legal bem definido" existindo ainda muitas zonas cinzentas sendo necessário continuar a adaptar o quadro legal ao "crescente protagonismo deste" DO (EMGFA, 2019a, pp. B-19).

2.2. Ambiente interno

Foi considerado pertinente a caracterização do ambiente interno das FFAA, investigando a situação atual através das perspetivas genética, estrutural e operacional[14], tendo recorrido a análise documental e a entrevistas a especialistas na área.

2.2.1. Perspetiva Genética

Não existe doutrina estruturante nas FFAA utilizando-se doutrina americana e NATO, estando neste momento em desenvolvimento a Estratégia Nacional de Ciberdefesa (ENCD) (Marques, 2019) (Rosa, 2019).

Em termos de formação e treino, tem-se verificado um cuidado do CCD para que haja formação comum e economia de escala, não existindo um *job description*. Existe ainda formação dispersa nos ramos, não havendo contudo formação de base existindo apenas duas pós-graduações (EMGFA, 2019a, p. 5) (Rosa, 2019) (Alexandre, 2019).

[14] *Vide* Anexo A.

O CCD tem adquirindo plataformas iguais ou interoperáveis devendo existir "políticas de *procurement*" e a garantia que o equipamento adquirido se encontra "na lista de material aprovado ou pela NATO ou pela UE" (Marques, 2019, pp. 9-10).

Foi identificada uma falta de centralização na captação de RH, porque senão "andam-se a canibalizar uns aos outros" (EMGFA, 2019a) (Marques, 2019, p. 15).

Existe a necessidade de adaptação das IE do CCD para acomodar as novas capacidades, estando para isso previsto mais um piso do EMGFA (Carvalho, 2019).

2.2.2. Perspetiva Estrutural

Existem diversas táticas, técnicas e procedimentos (TTP) encontrando-se desatualizadas e não harmonizadas devendo-se verificar quais as *best practice* atualmente implementadas na *National Institute of Standards and Technology* (NIST), na NATO ou nos Estados Unidos da América (EUA) (EMGFA, 2019a) (Alexandre, 2019).

Os núcleos CIRC têm Quadros Orgânicos (QO) diferentes e nem todos possuem a capacidade CERTDEF[15] preconizada, verificando-se que todos eles têm insuficiência de RH (Figura 21).

Existe a necessidade de rentabilizar o "investimento em formação" nos RH estando previsto um "período de inamovibilidade" no CCD e identificadas algumas contingências referentes à carreira (EMGFA, 2019a, p. 12).

	CIRC			Observações		
	O	S	P			
MARINHA						
Previsto	3	3	6	Total (previsto) = 12		
Existente	3	2	0	Total (Existências) = 5		
Diferencial	0	-1	-6	Total (diferença) = **-7**		**58,33%**
EXÉRCITO						
Previsto	5	6	3	Total (previsto) = 14		
Existente	3	1	0	Total (Existências) = 4		
Diferencial	-2	-5	-3	Total (diferença) = **-10**		**71,43%**
FORÇA AÉREA						
Previsto	7	5	-	Total (previsto) = 12		
Existente	5	0	-	Total (Existências) = 5		
Diferencial	-2	-5	-	Total (diferença) = **-7**		**58,33%**
			Total previsto	**38**		
			Total existente	**14** (36,84%)		
			Total em falta	**24 (63,16%)**		

Figura 21 – Relação pessoal CIRC ramos

[15] Capacidade permanente (24x7) de manter a estrutura de segurança e defesa do ciberespaço e da informação dos ramos.

2.2.3. Perspetiva Operacional

"Não existe doutrina operacional para a condução de operações militares no ciberespaço", nomeadamente *Standing Operating Procedures* (SOP) e TTP específicas, apenas "para dar resposta às necessidades de operações diárias" para "resposta de incidentes de segurança da informação" existindo nos EUA e na NATO alguma doutrina operacional (EMGFA, 2019a, p. 13) (Rosa, 2019).

Existe treino interno e treino conjunto mormente em exercícios nacionais e internacionais (Figura 22) denotando-se falta de interoperabilidade (IO) pessoal, havendo uma maior IO tecnológica, sendo um passo importante avançar para uma estrutura de rede da Defesa e não de redes segmentadas com uma interligação (EMGFA, 2019a) (Rosa, 2019) (Carvalho, 2019) (Alexandre, 2019).

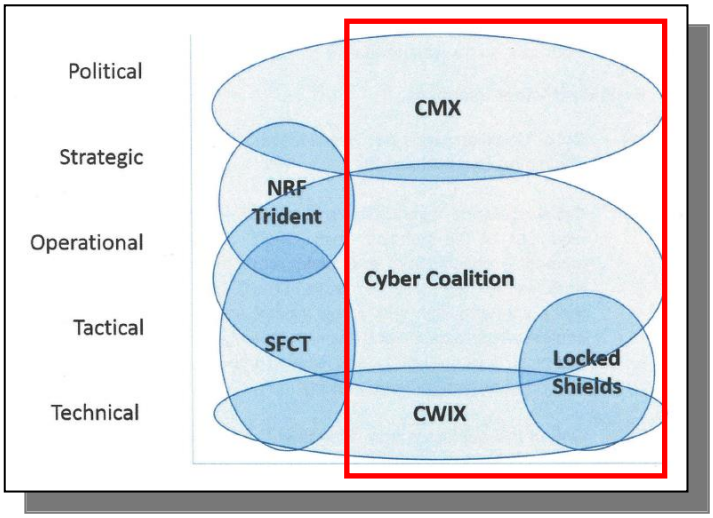

Figura 22 – Exercícios NATO em que Portugal participa

Fonte: (EMGFA, 2019a)

2.3. Síntese Conclusiva

Na análise do ambiente externo (Figura 23), verificou-se que decorrente da evolução do ciberespaço ocorreram diversos incidentes com implicações (mais ou menos graves) nas estruturas estatais. Foram encetadas diversas iniciativas NATO/UE e nacionais. Existe o aumento da economia cibernética que, aliada à denominada IoT/IoE emanam novas capacidades e consequentes riscos, sendo necessário efetuar sensibilização, nomeadamente junto dos serviços essenciais nacionais. Decorrente de toda esta mudança houve a necessidade da criação de legislação. Mas tudo isto implica *manpower*, denotando-se uma grande falta de RH.

A nível do ambiente interno (Figura 24), verificam-se lacunas nos vários níveis de doutrina, falta de centralização na captação de RH, havendo a necessidade da rentabilização da formação dos mesmos. A nível dos CIRC, verifica-se que possuem QO não normalizados, com lacunas de RH e sem capacidade CERTDEF. Caracterizou-se o ambiente cibernético nas dimensões propostas e correspondentes indicadores, pelo que se considera respondida a QD1, atingindo-se o OE1.

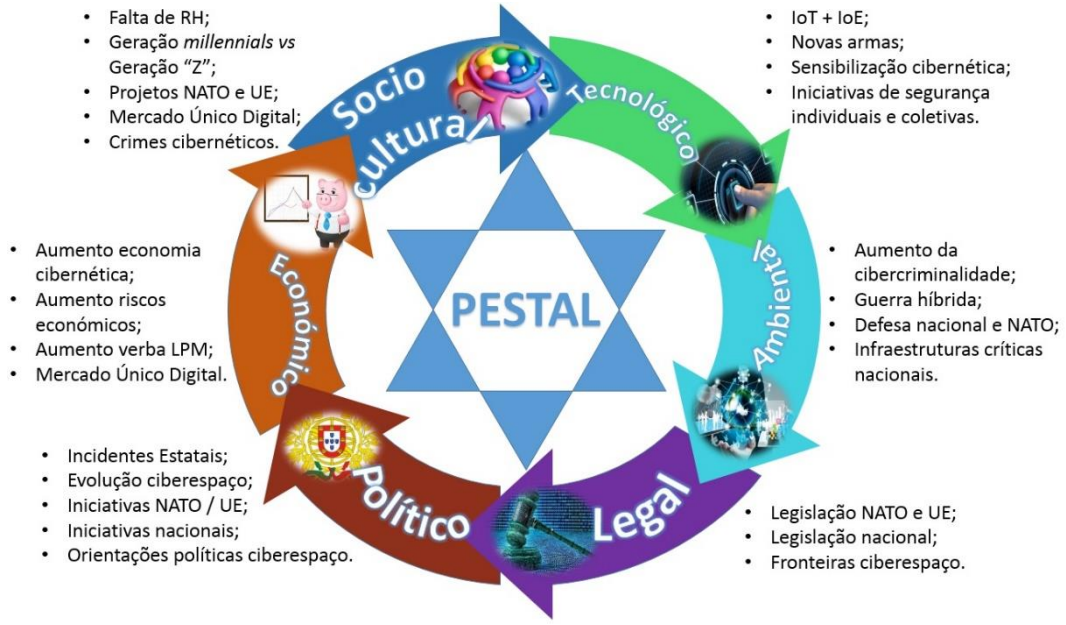

Figura 23 – Análise ambiente externo

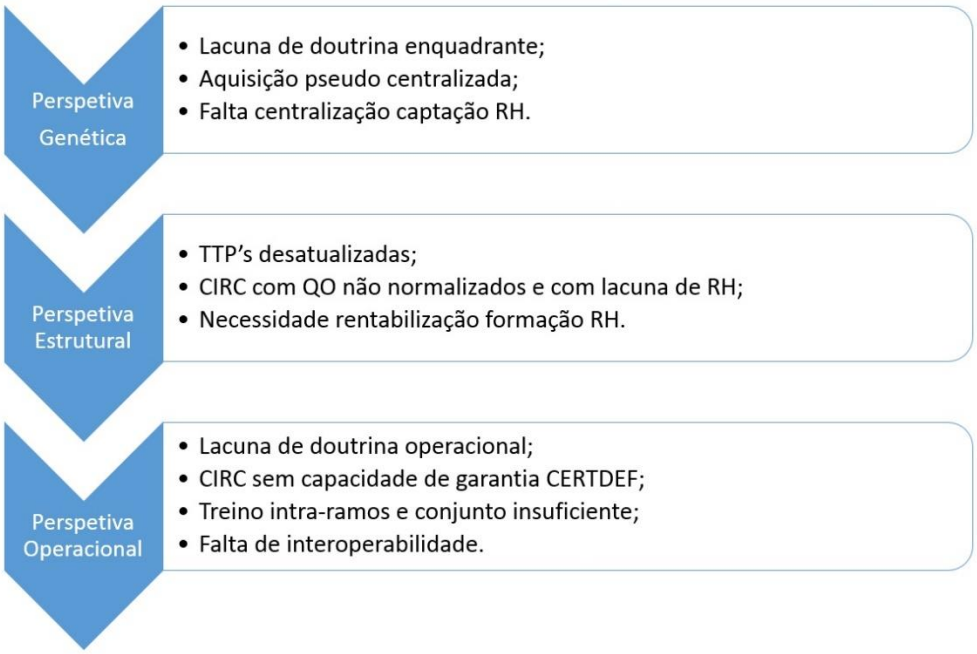

Figura 24 – Análise ambiente interno

3. Modelos dos núcleos CIRC

Neste capítulo pretende-se caracterizar os dois modelos escolhidos, verificando as vantagens e desvantagens dos mesmos, de modo a responder à QD2, atingindo o OE2.

A caracterização de cada um dos modelos será efetuada tendo em consideração a necessidade de levantamento de uma capacidade, baseado nos vetores DOTMLPII[16] definidos pela NATO (NATO, 2016, p. 3).

3.1. Modelo descentralizado

Este modelo é o que se encontra atualmente em vigor nas FFAA portuguesas, bem como em diversos outros países. Referindo-me especificamente às nossas FFAA, existe um núcleo CIRC em cada ramo das FFAA.

Existe doutrina em cada núcleo que se encontra desatualizada. Devido a esse facto os núcleos socorrem-se de doutrina NATO, americana e da NIST que são doutrinas diferentes e que são usadas de forma não uniforme pelos núcleos (Rosa, 2019) (Alexandre, 2019).

Verificou-se que cada núcleo possui a sua própria organização e detalhe sendo diferenciados uns dos outros, bem como a nível de quantitativos e sua distribuição (oficiais, sargentos e praças). Este modelo permite maior proximidade com a administração dos sistemas de cada ramo.

Em termos de formação e treino, não existe um *job description* para cada cargo nem um plano de formação comum ficando por vezes sujeitos ao financiamento de cada ramo e à formação disponibilizada através do CCD, estando neste momento a desenvolver-se um plano de formação. Existe algum treino específico que é efetuado em cada núcleo e existe treino conjunto que só é possível efetuar aquando de exercícios comuns (Rosa, 2019) (Jesus & Assunção, 2019).

Verifica-se que as plataformas existentes são comuns, adquiridas pelo CCD (sendo, no entanto, adquiridas quatro plataformas iguais) ou quando adquiridas pelos ramos, são interoperáveis com as outras. Contudo, deveria haver normas de *procurement* comuns e listas de *approved material*, em conformidade com as necessidades NATO e da UE (Marques, 2019) (Castro, 2019).

Neste modelo, o chefe de cada núcleo é um oficial superior (CTEN/MAJ) que se encontra sob a dependência hierárquica das Tecnologias de Informação e Comunicações (TIC) de cada ramo, verificando-se uma preocupação dos ramos em manter essa valência.

[16] Do original em inglês DOTMLPFI – *Doctrine, Organisation, Training, Material, Leadership development, Personnel, Facilities and Interoperability*. *Vide* Anexo A.

Pode-se considerar que existe uma relação técnica entre os CIRC e o CCD, relação essa não institucionalizada.

Nenhum dos núcleos tem a lotação completa, faltando em cada um mais de 50% dos efetivos. Decorrente da obrigatoriedade de rotação de pessoal, normal nos ramos, e da necessidade de garantir determinadas condições para promoção, os RH com formação e treino são afastados dos cargos perdendo-se valências importantes (Rosa, 2019).

Todos os núcleos possuem IE que cumprem com os requisitos de segurança necessárias, quer a nível físico quer a nível de ligações de segurança.

Decorrente das entrevistas efetuadas, verifica-se que já existe uma preocupação em garantir que os sistemas são interoperáveis, considerando-se, no entanto, que existe uma maior dificuldade na partilha de informação e algum desconhecimento, o que dificulta a IO.

3.2. Modelo centralizado

Consta de um modelo no qual existe apenas um núcleo CIRC nas FFAA, à semelhança do existente na Holanda, que no caso português ficaria na dependência do CCD. Foi escolhido o modelo da Holanda, devido ao facto de ser um membro NATO, aliado à semelhança dimensional entre FFAA .

Existe, analogamente ao modelo descentralizado, a necessidade de haver doutrina estruturante, e doutrina específica para os ramos, TTP e SOP com as especificidades necessárias. Como estaria centralizado, a doutrina comum seria atualizada mais facilmente e seria uniforme, facilitando a criação de doutrina específica (Carvalho, 2019).

Em termos de organização, ficaria na dependência do CCD com *Rapid Response Teams* (RRT) nos ramos, seja em permanência para os ramos manterem alguma valência, seja *case by case*, apenas em caso de necessidade.

Neste modelo, existe igualmente a necessidade de haver um *job description* para cada cargo e um plano de formação. No entanto não estariam sujeitos à disponibilidade de financiamento dos ramos, apenas do EMGFA, que é quem tem verba alocada para a CD conforme constante na LPM (LO 2/2019, 2019), ganhando-se economia de escala pois os cursos nesta área são bastante dispendiosos (NCIA, 2020) (SANS, 2020). Seria importante garantir treino específico de cada ramo, inclusive junto dos utilizadores. As plataformas seriam comuns e ganhar-se-ia na aquisição das mesmas (usando as normas de *procurement* comuns e listas de *approved material*), pois não seria necessário adquirir tanta quantidade.

O chefe do CIRC da defesa provavelmente seria um CFR/TCOR, em regime de rotatividade entre os ramos. Em termos de quantitativos, seriam os necessários para garantir CERTDEF (conforme preconizado no modelo atual, não sendo possível garantir), bem como a existência de RRT, prevendo-se a alocação de menos RH, libertando alguns para outras funções no CCD. Será importante maximizar a rentabilização dos RH, prever condições para a progressão vertical e para a progressão horizontal a partir de determinado posto e de maior permanência na área da CD, potenciando as suas valências e o investimento efetuado.

Poderiam ser utilizadas as IE do CCD ou outras, desde que todo o CIRC e de preferência, todo o CCD esteja junto pois a nível de CD funciona muito em fóruns de equipas, partilhando ideias e experiências. No caso de se utilizarem outras instalações que não as do CCD, possivelmente seria necessário adaptar as mesmas, garantindo as necessárias condições de segurança (Teixeira, 2020).

Neste modelo a IO seria potenciada, aumentando a cooperação, colaboração e partilha. O facto dos elementos trabalharem juntos potencia a confiança entre os membros dos diversos ramos, sendo, no entanto, mais difícil manter uma estreita relação entre as diversas unidades nos ramos e o CIRC.

3.3. Vantagens e desvantagens

Através do recurso a entrevistas, sua posterior validação e análise[17], foram identificadas diversas vantagens e desvantagens em ambos os modelos.

Verificou-se que o modelo centralizado potencia a harmonização da doutrina e a poupança de RH alocados à atualização da mesma, sendo necessário garantir doutrina tática, própria de cada ramo. Facilita a integração da CD em operações e exercícios conjuntos, promove uma formação centralizada, uniforme e com maior economia de escala podendo, no entanto, haver um maior afastamento entre o núcleo e os utilizadores. Fomenta a segurança das redes devido ao facto do modelo atual não garantir o CERTDEF, bem como a poupança de recursos económicos com a aglutinação de plataformas e eliminação de redundâncias.

O modelo descentralizado, terá uma maior aceitação pelas chefias dos ramos pelo facto de quererem manter essa valência no ramo. No entanto, existe a necessidade de mais RH, um recurso escasso atualmente. Este modelo utiliza as IE já existentes, no entanto, dificulta a IO.

[17] *Vide* Apêndice B.

3.4. Síntese Conclusiva

Foram identificados 29 indicadores, repartidos em vantagens e desvantagens (Figura 26), realçando-se que o modelo centralizado potencia a existência de doutrina, de *best practices*, taxonomia comuns e criação de SOP e TTP, uma formação centralizada e uniformizada, maior facilidade na garantia CERTDEF, eficiência de RH e de processos, potenciando a partilha de informação e aumentando a IO.

Referente ao modelo descentralizado, evidenciam-se como vantagens, uma maior proximidade intra-ramo e a utilização das IE já existentes diminuindo possíveis custos.

Verifica-se que o modelo centralizado apresenta mais vantagens (75,9%), conforme Figura 25, repartidas pelos diversos indicadores, apresentando-se como tendo mais potencialidades para contribuir para a edificação de uma capacidade, sendo assim respondida a QD2, atingindo-se o OE2.

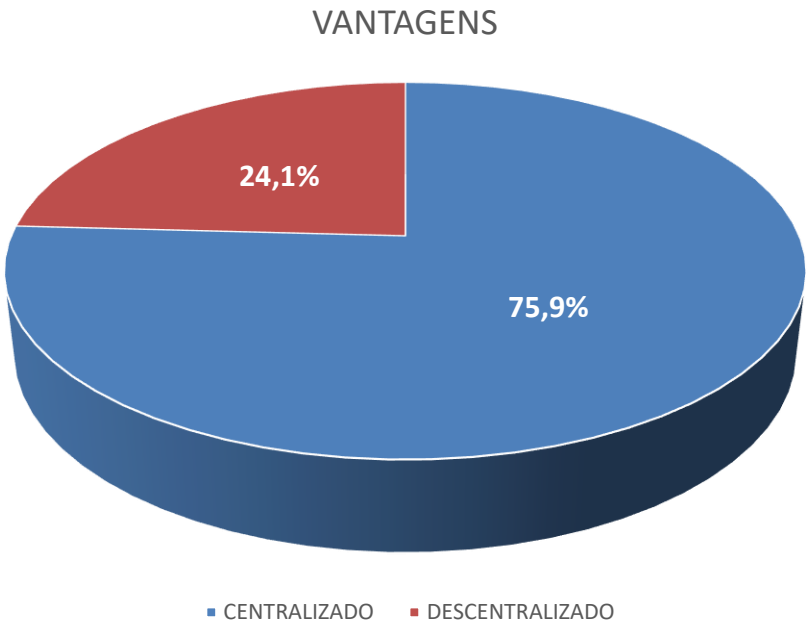

Figura 25 – Percentagem das vantagens de cada modelo

MODELO DESCENTRALIZADO	MODELO CENTRALIZADO
DOUTRINA	
⬇Doutrina mais dispersa, divergente e menos normalizada; ⬇Mais RH alocados à atualização da doutrina; ⬆Manutenção de alguma identidade própria de cada ramo.	⬆Potencia harmonização da doutrina e de *best practices* comuns, taxonomia comum e criação de SOP e TTP; ⬆Poupança de RH na atualização da doutrina; ⬇Pode-se perder alguma taxonomia própria dos ramos.
ORGANIZAÇÃO	
⬇Maior dificuldade na integração da componente cibernética nas operações conjuntas; ⬇Capacidade de resposta dificultada; ⬆Inicialmente maior facilidade nas operações específicas de cada ramo; ⬆Ausência de dificuldade organizacional da parte das chefias; ⬇Menor uniformidade na obtenção de RH.	⬆Facilita a integração da componente cibernética nas operações conjuntas; ⬆Potencia a capacidade de resposta; ⬇Maior dificuldade inicial nas operações específicas de cada ramo; ⬇Apresenta como desafio organizacional o ego das chefias; ⬆Maior uniformidade na obtenção de RH.
TREINO	
⬇Existência de formação dada pelos ramos em vez de ser toda centralizada e uniformizada; ⬇Alguma formação diferente entre os ramos; ⬆Maior proximidade dentro de cada ramo; ⬇Menor capacidade para fornecer formação e treino; ⬇Dificulta a economia dos números na formação.	⬆Formação centralizada e uniformizada; ⬆Formação obtida através duma matriz de formação (*road map*); ⬇Menor proximidade dentro de cada ramo; ⬆Maior capacidade para fornecer formação e treino; ⬆Potencia a economia dos números na formação.
MATERIAL	
⬇Maiores gastos de recursos económicos com aquisição de plataformas; ⬇Potencia redundâncias desnecessárias entre os ramos; ⬇Aquisição de plataformas de treino e de ciberdefesa descentralizada.	⬆Poupança de recursos económicos (aglutinação de plataformas); ⬆Elimina redundâncias desnecessárias; ⬆Assegura a normalização na aquisição de plataformas de treino e de ciberdefesa.
LIDERANÇA	
⬆Aceitação pelas lideranças facilitada; ⬆Ausência da necessidade de desprendimento.	⬇Dificuldade de aceitação pelas lideranças (necessidade de mentalização); ⬇Falta de confiança e de desprendimento.
PESSOAL	
⬇Incapacidade de garantir a CERTDEF; ⬇Necessidade de mais RH; ⬇Mais recursos monetários na contratação de RH civis; ⬇Mais gastos na retenção de RH civis; ⬇Menor eficácia e eficiência.	⬆Maior facilidade na garantia da CERTDEF; ⬆Menos RH para garantir as mesmas valências; ⬆Menor necessidade de contratação de RH civis; ⬆Menos gastos na retenção de RH civis; ⬆Potencia a eficácia e eficiência dos processos.
INFRAESTRUTURAS	
⬆Utilização de infraestruturas já existentes; ⬇Menor interoperabilidade com descentralização; ⬇Menor resiliência das redes existindo um domínio único.	⬇Necessidade de acomodar mais RH no mesmo espaço; ⬆Centralização potencia a interoperabilidade; ⬆Maior resiliência das redes existindo um domínio único.
INTEROPERABILIDADE	
⬇Dificulta a partilha de informação; ⬇Maior filtragem na partilha de informação; ⬇Dificulta a interoperabilidade (tecnológica, técnica e pessoal).	⬆Potencia a partilha de informação; ⬆Menor filtragem na partilha de informação; ⬆Aumenta a interoperabilidade (tecnológica, técnica e pessoal).

Figura 26 – Vantagens e desvantagens dos modelos CIRC

4. Contributos para a edificação da capacidade de CD

Neste capítulo procurar-se-á verificar qual o modelo que melhor contribui para o desenvolvimento da capacidade acima referida, tendo em consideração o ambiente atual (interno e externo), os modelos preconizados e as Linhas de Ação (LA) estratégicas.

4.1. Corelacionamento dos modelos CIRC com as LA

Decorrente do "Plano", foram definidas LA estratégicas organizadas segundo os vetores DOTMLPII, interligando-as com o Mapa da Estratégia para a CD (Figura 27).

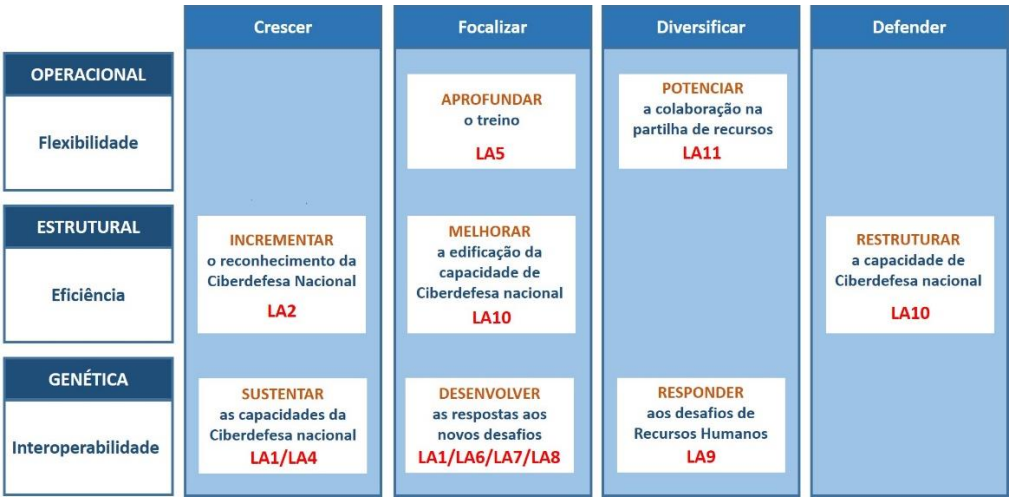

Figura 27 – Mapa da Estratégia da CD

Fonte: Adaptado de: (EMGFA, 2019b, p. 10)

Após analisadas as LA referidas anteriormente, elaboraram-se entrevistas a peritos e intervenientes diretos em CD/CS, verificando-se que os modelos poderiam interferir, direta ou indiretamente nas seguintes LA.

- LA 1 – "Criar uma base doutrinária para a Ciberdefesa a nível nacional, enquadrada pelo normativo das organizações a que Portugal pertence" (EMGFA, 2019b, p. 14), nomeadamente A1.02, 1.03 e 1.04. Para a uniformização da elaboração, desenvolvimento e atualização da doutrina operacional e tática para a CD, considerou-se o modelo centralizado, havendo uma camada comum de legislação, o que facilita a elaboração e implementação de SOP e TTP necessárias.

- LA 2 – "Adequar a estrutura orgânica da Ciberdefesa nacional e as suas relações organizacionais face às novas solicitações" (EMGFA, 2019b, p. 15), nomeadamente A2.02 e 2.03. Foi considerado o modelo centralizado como o que melhor contribui para a integração

da componente cibernética nas operações conjuntas. No entanto é necessário acautelar as especificidades decorrentes das operações específicas dos ramos.

- LA 4 – "Dinamizar a educação e formação em Ciberdefesa" (EMGFA, 2019b, p. 17), nomeadamente A4.03. Verifica-se que o modelo centralizado contribui para uma formação uniforme ganhando economia de escala e não estando essa mesma formação sujeita à disponibilidade cedida pelo EMGFA, nem a restrições orçamentais, já que os ramos não possuem verba alocada especificamente para a CD como o EMGFA, através da LPM. No entanto, no que concerne à sensibilização, o modelo descentralizado é o que melhor contribui, devido à proximidade existente entre os núcleos CIRC dos ramos e os administradores de redes e utilizadores dos ramos.

- LA 6 – "Modernizar e sustentar os parques informáticos e as soluções tecnológicas das redes da Defesa Nacional" (EMGFA, 2019b, p. 18), nomeadamente A6.01 e 6.02. Neste ponto existe uma grande divisão de opiniões. Por um lado, é considerado que mais importante que o modelo adotado seria importante possuir uma só rede da Defesa, em vez de uma série de redes unificadas. No entanto, é igualmente considerado o modelo centralizado, pois seria mais fácil de implementar políticas de *procurement* e de aquisição, bem como, devido ao facto dos responsáveis pela segurança não deverem estar sob a chefia do responsável pela gestão das redes. No que concerne à harmonização de soluções tecnológicas é defendido o modelo centralizado por facilitar a homogeneidade (apesar desta já existir parcialmente, devido à aquisição de plataformas efetuada pelo EMGFA) e permitir a aglutinação de plataformas.

- LA 7 – "Garantir a evolução futura das soluções tecnológicas para a Ciberdefesa nacional" (EMGFA, 2019b, p. 19), nomeadamente A7.01 e 7.03. Tal como na LA anterior, foi considerado o modelo centralizado pois permite aquisição uniforme e em menor escala o que permitiria uma poupança de recursos devido ao elevado preço destas plataformas.

- LA 8 – "Satisfazer a resposta estrutural e operacional da Ciberdefesa nacional face aos desafios futuros" (EMGFA, 2019b, p. 20). Referente a esta LA, o modelo descentralizado foi considerado como sendo aquele que terá melhor aceitação pela liderança, pois os ramos pretendem manter a valência que possuem, sendo uma questão de interesses e de orientações político-estratégicas. No entanto, com uma estrutura conjunta recetiva a requisitos dos ramos aliada à perspetiva de rentabilização de recursos, poderá fazer com que a aceitação do modelo conjunto seja maior. Até porque devemos "juntar todas as nossas capacidades, as nossas competências e recursos para criarmos (…) condições para que

Portugal possa proteger aquilo que é verdadeiramente crítico para o funcionamento do país" (Ribeiro, 2019).

- LA 9 – "Adequar a realidade dos recursos humanos afetos à Ciberdefesa para os desafios futuros" (EMGFA, 2019b, p. 13). Os RH especializados em CD são sem dúvida uma grande preocupação em ambos os modelos. Os ramos e o EMGFA têm de agir segundo as mesmas diretrizes e orientações políticas prevenientes do Ministério da Defesa Nacional (MDN). Desta forma foram identificadas algumas iniciativas importantes a considerar. No respeitante à gestão de carreiras, deverá haver uma permanência prolongada dos RH afetos a esta área, com uma carreira aliciante e desafiante, com a possibilidade de manutenção na área durante toda a carreira. Para tal é necessário garantir um conjunto de cargos que garantam uma progressão de carreira até ao topo (no próprio ramo, no CCD, na NCIA e no CNCS). Eventualmente, pela impossibilidade de garantir essa progressão vertical a todos, deve-se prever a progressão mista. Dever-se-á considerar a implementação da classe de sargentos e de praças, bem como a especialização de oficiais em CD.

Referente à obtenção de RH, um dos pontos essenciais é o vencimento que, face aos auferidos no mundo civil será difícil de igualar. Torna-se importante aliciar os recém-formados logo à saída (ou mesmo durante o decorrer do curso, através da frequência de estágios) dos politécnicos, das universidades, dos Institutos de Emprego e Formação Profissional (IEFP) ou através da mobilidade interna na Administração Pública (AP). Inclusive, patrocinar formação superior garantindo a sua permanência nas FFAA durante um período de tempo após a conclusão da formação.

Face ao exposto considera-se que o modelo centralizado, que requer menos recursos, com um *procurement* centralizado seria o melhor pois "se não for assim, andam-se a canibalizar uns aos outros" (Marques, 2019, p. 15).

- LA 10 – "Consolidar as condições de utilização da capacidade da Ciberdefesa nacional" (EMGFA, 2019b, p. 23). Apesar dos núcleos CIRC terem IE com as necessárias condições de segurança, é importante a estrutura de CD funcionar de forma unificada, evidenciando uma preferência pelo modelo centralizado, de modo a haver uma maior partilha de conhecimento, podendo-se para tal (perspetivando a deslocalização do EMGFA das atuais instalações fruto da "alienação do atual edifício, no Restelo, que alberga atualmente os serviços da Defesa Nacional e o" EMGFA), pensar uma IE de raiz, com todas as condições necessárias, podendo albergando igualmente os restantes *players* da CS/CD

nacional, mesmo que se mantenham "com as dependências hierárquicas" atuais (Governo, 2019) (Marques, 2019, p. 16).

- LA 11 – "Dinamizar os processos de interoperabilidade da Ciberdefesa com atores externos" (EMGFA, 2019b, p. 23), nomeadamente A11.01, 11.02 e 11.03. O modelo centralizado, pelo simples facto de estarem reunidos no mesmo local, otimiza o processo de partilha de informação reduzindo a quantidade de barreiras invisíveis existentes.

4.2. Síntese Conclusiva

Decursivo das respostas às QD foi possível elaborar duas matrizes SWOT[18] (Figuras 28 e 29), identificando as LA que promovem cada um dos parâmetros definidos (crescimento, focalização, diversificação e defesa).

	AMBIENTE INTERNO	
AMBIENTE EXTERNO	**POTENCIALIDADES** 1. Manutenção de identidade de cada ramo; 2. Inicialmente maior facilidade nas operações específicas de cada ramo; 3. Dificuldade organizacional diminuta; 4. Maior proximidade inter-ramos; 5. Aceitação pelas lideranças; 6. Ausência da necessidade de desprendimento; 7. Utilização de infraestruturas já existentes.	**VULNERABILIDADES** 1. Doutrina dispersa, divergente e menos normalizada; 2. Dificuldade na integração da componente cibernética nas operações conjuntas; 3. Maior dificuldade na obtenção de RH; 4. Formação descentralizada e não uniformizada; 5. Menor capacidade para fornecer formação e treino aos utilizadores das unidades; 6. Dificulta a economia dos números na formação; 7. Dificulta a segurança das redes; 8. Maiores gastos de recursos económicos com aquisição de plataformas; 9. Potencia redundâncias desnecessárias; 10. Aquisição de plataformas de treino e de CD descentralizada; 11. Incapacidade de garantir a CERTDEF; 12. Necessidade de mais RH; 13. Maior uniformidade na contratação de RH civis; 14. Gastos na retenção de RH civis; 15. Menor eficácia e eficiência; 16. Menor resiliência das redes; 17. Maior filtragem na partilha de informação; 18. Dificulta a interoperabilidade (tecnológica, técnica e pessoal).
OPORTUNIDADES 1. Projeto *MultiNational Cyber Defence on Education and Training* (MN CD E&T); 2. Edificação do *Cyber Academia and Innovation Hub* (Academia Militar) e da NCIA (Oeiras); 3. CD como área prioritária pelo Governo e pela NATO; 4. RH motivados; 5. Criação do *Campus* da Defesa; 6. Partilha de informação, recebendo *best practices;* 7. Aplicabilidade do Direito Internacional à CD.	**CRESCIMENTO** • Potenciar a harmonização organizacional; • Promover o investimento em CD.	**FOCALIZAÇÃO** • Elaborar e harmonizar doutrina de CD entre a NATO e os ramos; • Efetuar e fortalecer protocolos com entidades civis (públicas e privadas) nacionais; • Fortalecer parcerias com a NATO; • Harmonizar os requisitos de formação com as *best practice* externas; • Potenciar parcerias no âmbito da formação e treino; • Criar regulamentação comum de segurança de redes; • Criar lista de *approved material* e de políticas de *procurement.* **LA 8 - Satisfazer a resposta estrutural e operacional da Ciberdefesa nacional face aos desafios futuros**
AMEAÇAS 1. Criminalidade cibernética; 2. Aumento riscos económicos decorrentes de ciberataques; 3. Alterações orçamentais desfavoráveis; 4. Ciberespaço privilegiado para ataques assimétricos; 5. Aumento capacidade cibernética países não aliados; 6. Parcerias insuficientes e deficitárias; 7. Falta de RH; 8. Dificuldade de recrutamento de civis.	**DIVERSIFICAÇÃO** • Dremir riscos em cada rede das FFAA; • Elaborar procedimentos de resposta a ciberameaças comum aos ramos; • Criar condições de diminuição de riscos económicos decorrentes de ciberataques; • Garantir a evolução das soluções tecnológicas existentes; • Aumentar a capacidade de CD nacinal. **LA 4 - Dinamizar a educação e formação em Ciberdefesa**	**DEFESA** • Integrar todas as redes da Defesa nas plataformas de monitorização; • Integrar a componente cibernética nas operações comuns e específicas dos ramos; • Dinamizar o treino conjunto; • Propor condições específicas para os RH civis a integrar nas FFAA; • Potenciar condições para a retenção dos RH nas FFAA.

Figura 28 – Matriz SWOT – Modelo Descentralizado

Fonte: Adaptado de: (EMGFA, 2019b, p. 9)

[18] *Strengths*, *Weaknesses*, *Opportunities*, *Threats*; *Vide* Anexo A.

	AMBIENTE INTERNO	
AMBIENTE EXTERNO	**POTENCIALIDADES** 1. Harmonização da doutrina e de *best practices* comuns e criação de SOP e TTP; 2. Poupança de RH; 3. Integração da componente cibernética nas operações conjuntas; 4. Facilidade na obtenção de RH; 5. Potencia a capacidade de resposta; 6. Formação centralizada e uniformizada (*road map*); 7. Maior capacidade para fornecer formação e treino aos utilizadores das unidades; 8. Potencia a economia dos números na formação; 9. Garante maior segurança das redes; 10. Poupança de recursos económicos, aglutinação de plataformas eliminando redundâncias desnecessárias; 11. Normalização na aquisição de plataformas de treino e de CD; 12. Facilidade na garantia da CERTDEF; 13. Menor necessidade de contratação de RH civis; 14. Menos gastos na retenção de RH civis; 15. Maior eficácia e eficiência dos processos; 16. Potencia a interoperabilidade; 17. Maior resiliência das redes existindo um domínio único; 18. Potencia a partilha de informação; 19 . Menor filtragem na partilha de informação; 20. Menor contacto com as unidades nos ramos; 21. Maior interoperabilidade (tecnológica, técnica e pessoal).	**VULNERABILIDADES** 1. Perda de taxonomia própria de cada ramo; 2. Dificuldade inicial nas operações específicas de cada ramo; 3. Desafio organizacional/aceitação pelas lideranças - gestão de egos; 4. Menor proximidade intraramos; 5. Falta de confiança e de desprendimento; 6. Mais RH no mesmo espaço.
OPORTUNIDADES 1. Projeto *MultiNational Cyber Defence on Education and Training* (MN CD E&T); 2. Edificação do *Cyber Academia and Innovation Hub* (Academia Militar) e da NCIA (Oeiras); 3. CD como área prioritária pelo Governo e pela NATO; 4. RH motivados; 5. Criação do *Campus* da Defesa; 6. Partilha de informação, recebendo *best practices;* 7 . Aplicabilidade do Direito Internacional à CD.	**CRESCIMENTO** • Harmonizar doutrina nacional (estratégica, tática e operacional) com a doutrina nacional de CS e com a doutrina internacional de CD; • Incrementar e fortalecer sinergias com parceiros nacionais e internacionais; • Harmonizar os requisitos de formação com as *best practice* externas; • Potenciar parcerias âmbito formação e treino CCD/NCIA; • Recrutar RH motivados; • Dinamizar intercâmbio de RH; • Garantir evolução concertada dos conhecimentos internos. **LA 1 - Criar um edifício doutrinário para a Ciberdefesa a nível nacional.** **LA 7 - Garantir a evolução futura das soluções tecnológicas para a Ciberdefesa nacional.**	**FOCALIZAÇÃO** • Elaborar doutrina comum para os ramos; •Implementar processo de avaliação dos riscos das redes de defesa nacionais; • Criar condições para o recrutamento de RH especializados; • Criar regulamentação para carreiras horizontais; • Criar especialidade CD comum aos ramos; • Potenciar a consciencialização das chefias para a necessidade de uma solução concertada e comum; • Criar ligação estreita entre o CCD e os utilizadores/ADU dos ramos; • Adequar a estrutura do CCD para albergar CIRC comum. **LA 6 - Modernizar e sustentar os parques informáticos e as soluções tecnológicas das redes da Defesa Nacional** **LA 10 - Consolidar as condições de utilização da capacidade da Ciberdefesa nacional**
AMEAÇAS 1. Criminalidade cibernética; 2. Aumento riscos económicos decorrentes de ciberataques; 3. Alterações orçamentais desfavoráveis; 4. Ciberespaço privilegiado para ataques assimétricos; 5. Aumento capacidade cibernética países não aliados; 6. Parcerias insuficientes e deficitárias; 7. Falta de RH; 8. Dificuldade de recrutamento de civis.	**DIVERSIFICAÇÃO** • Potenciar cooperação com aliados e organizações nacionais e internacionais de forma a colmatar falhas; • Elaborar doutrina operacional; • Dinamizar recrutamento externos junto de universidade e Centros de Formação; • Potenciar e alargar parcerias existentes com parceiros nacionais e internacionais. **LA 4 - Dinamizar a educação e formação em Ciberdefesa** **LA 9 - Adequar a realidade dos recursos humanos afetos à Ciberdefesa para os desafios futuros** **LA 11 - Dinamizar os processos de interoperabilidade da Ciberdefesa com atores externos**	**DEFESA** • Integrar todas as redes da Defesa nas plataformas de monitorização; • Elaborar doutrina estratégica e operacional das FFAA; • Integrar a componente cibernética nas operações comuns e específicas dos ramos; • Dinamizar o treino conjunto; • Propor condições específicas para os RH civis a integrar nas FFAA; • Potenciar condições para a retenção dos RH nas FFAA. **LA 2 - Adequar a estrutura orgânica da Ciberdefesa nacional e as suas relações organizacionais face às novas solicitações**

Figura 29 – Matriz SWOT – Modelo Centralizado

Fonte: Adaptado de: (EMGFA, 2019b, p. 9)

Decorrente da análise documental e das entrevistas, considera-se que o modelo centralizado é aquele que apresenta mais potencialidades para contribuir positivamente para as LA1 (A1.02/A1.03/A1.04), LA2 (A2.02/A2.03), LA4, LA6 (A6.01/A6.02), LA7 (A7.01/A7.03), LA9, LA10 e LA11 (A11.01/A11.02/A11.03), conforme Figura 30. Considera-se assim respondida a QC atingindo-se o OG deste trabalho, evidenciando-se o modelo centralizado como aquele que potencialmente melhor contribui para a edificação da capacidade de CD nacional.

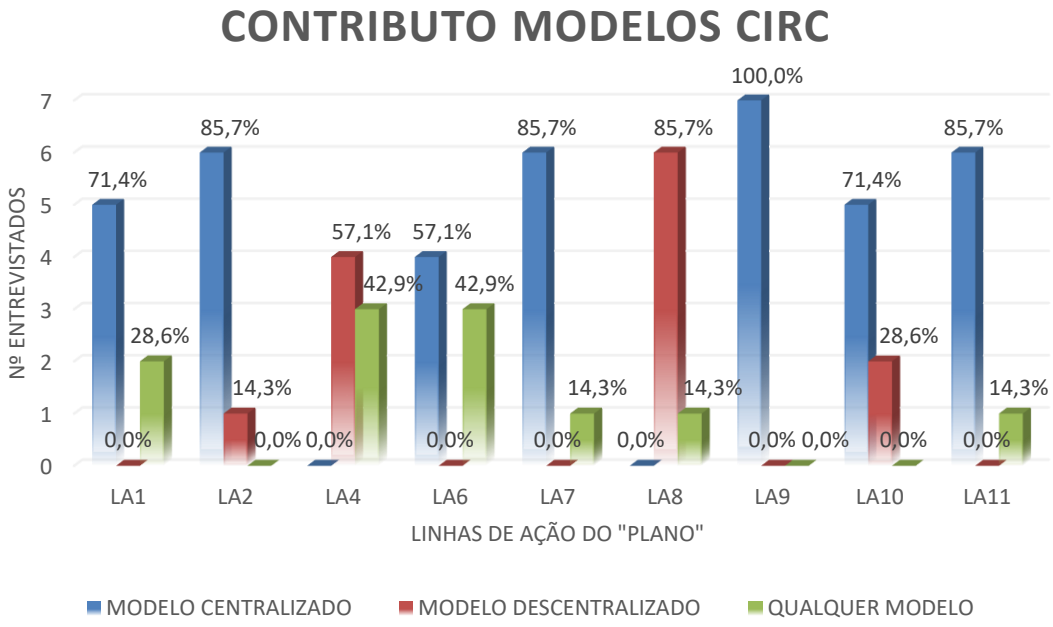

Figura 30 – Contributo para as LA do "Plano"

Conclusões

Assumiu-se neste trabalho uma ontologia construtivista, considerando-se que os fenómenos sociais são produzidos pela interação social estando em constante reconstrução, conforme evidenciado pela constante e célere alteração das atividades efetuadas no e através do ciberespaço, aliada a uma epistemologia interpretativista. Utilizou-se o raciocínio dedutivo, não se tratando da verdade dos factos, mas sim da sua validade, conjugado com o pensamento crítico, empregando-se uma estratégia de investigação mista.

Com o propósito de analisar o ambiente cibernético externo às FFAA, recorreu-se à análise PESTAL. Averiguou-se que apesar de encetadas iniciativas NATO/UE e nacionais, a rápida mudança/evolução do ciberespaço, aliada à crescente economia cibernética potenciou o aumento da cibercriminalidade podendo afetar os serviços essenciais nacionais, levando à necessidade de proteção das IE críticas criando uma lacuna de RH.

Caracterizou-se o ambiente interno, nas perspetivas genética, estrutural e operacional, no sentido de apurar a situação atual da CD nas FFAA. Realça-se a falta de doutrina, centralização na captação de RH e capacidade CERTDEF, aliada à escassez de RH especializados, sendo premente a rentabilização da formação dos mesmos.

A caracterização do ambiente cibernético possibilitou responder à QD1 atingindo-se o OE1.

Seguidamente caracterizaram-se os dois modelos CIRC preconizados, considerando a necessidade de edificação de uma capacidade, sustentada nos vetores DOTMLPII. Para tal utilizaram-se entrevistas aos intervenientes referidos e efetuou-se análise documental, obtendo as vantagens e desvantagens de cada um dos modelos. Das 29 vantagens encontradas, 22 encontravam-se associadas ao modelo centralizado (75,9%) evidenciando-se o mesmo como sendo aquele que melhor potencia a edificação de uma capacidade, respondendo-se assim à QD2 e atingindo-se o OE2.

Por fim, face ao atual ambiente cibernético e aos dois modelos alvitrados e face às LA do "Plano", devidamente correlacionadas com o Mapa da Estratégia da CD, foi possível averiguar quais as LA que cada modelo tem mais competências para potenciar, contribuindo para a edificação da capacidade de CD, respondendo à QC, atingindo assim o OG deste trabalho, obtendo os resultados descritos em seguida.

Entende-se, perante a análise documental, às respostas decorrentes das entrevistas e à comparação das duas matrizes SWOT, que o modelo centralizado é aquele que potencialmente mais contribui nas seguintes LA:

- LA 1: Criar uma base doutrinária para a CD a nível nacional, enquadrada pelo normativo das organizações a que Portugal pertence (Parcialmente verificada);

- LA 2: Adequar a estrutura orgânica da CD nacional e as suas relações organizacionais face às novas solicitações (Verificada);

- LA 4: Dinamizar a educação e formação em CD (Parcialmente verificada);

- LA 6: Modernizar e sustentar os parques informáticos e as soluções tecnológicas das redes da Defesa Nacional (Parcialmente verificada);

- LA 7: Garantir a evolução futura das soluções tecnológicas para a CD nacional (Verificada);

- LA 9: Adequar a realidade dos recursos humanos afetos à CD para os desafios futuros (Totalmente verificada);

- LA 10: Consolidar as condições de utilização da capacidade da CD nacional (Parcialmente verificada);

- LA 11: Dinamizar os processos de IO da CD com atores externos (Verificada) (Santos, et al., 2019, p. 142).

Os resultados deste trabalho contribuem para a melhoria do conhecimento sobre a matéria (uma vez que o "Plano", e as entrevistas efetuadas já contemplam alguns destes resultados), nomeadamente nos seguintes pontos:

- Melhoria da eficácia e eficiência no que alude ao desenvolvimento e atualização uniforme da doutrina afeta à CD;

- Definição de uma organização bem como de *job description* uniformes e comuns para cada cargo do CIRC (mantendo-se a configuração atual ou partindo-se para um modelo centralizado);

- Definição de um *road map* formativo coerente e consistente, e de políticas de *procurement*;

- Criação de uma lista de *approved material* que permita tratar de informação classificada (NATO e/ou UE);

- Incremento da IO entre os vários atores;

- Definição de políticas comuns de *procurement* de pessoal;

- Exploração de algumas iniciativas que poderão ser importantes para a gestão da carreira destes especialistas, bem como para a contratação de civis para a CD nas FFAA, sendo considerados os dois contributos mais marcantes pelo facto dos RH especializados em CD constituírem uma parte cruciforme nesta matéria, pela falta existente (nas FFAA e no mundo civil), e pelo custo inerente a essa especialização.

Considera-se que os resultados obtidos neste trabalho ainda carecem de estudos mais aprofundados para proceder à sua operacionalização, mormente no que concerne aos RH e às IE, pelo que se recomenda, no caso de se avançar para uma solução centralizada, que sejam desenvolvidos pelo EMGFA, através de um GT com elementos dos três ramos, para verificar a sua aceitabilidade, exequibilidade e adequabilidade, bem como, a melhor forma de os implementar.

Verificou-se igualmente que existem diversos aspetos que podem (ou mesmo devem) ser salvaguardados de modo a facilitar a integração dos CIRC num CIRC conjunto, formulando-se as seguintes recomendações:

- Criação de uma única rede da Defesa;

- Doutrina que contemple as especificidades das redes dos ramos, garantindo uma taxonomia comum;

- Pequena célula de CD nos comandos operacionais de cada ramo ou como alternativa, prever a utilização de elementos do CCD adstritos às operações e exercícios, quer comuns quer específicos de cada ramo;

- Garantia de RRT com elementos dos três ramos;

- Formação específica para as especificidades das redes de cada ramo;

- Recetividade a requisitos dos ramos;

- Garantia de redundância do local de monitorização da(s) rede(s) de modo a não comprometer a resiliência da(s) mesma(s);

- Existência de centros de monitorização das redes de cada ramo, sendo o visionamento ao nível do CIRC conjunto.

Fruto da delimitação da investigação aos modelos CIRC, poder-se-á ter limitado de alguma forma este trabalho pois excluiu-se o estudo da possibilidade da criação de um Comando de CD, como existe nos EUA, ou da criação de um ramo das FFAA, tal como existe na Alemanha (Comando do Ciberespaço e de Informação), que engloba a capacidade

cibernética, as tecnologias de informação, a *intelligence* e a geoinformação. Igualmente não se abordou a possibilidade, constrangimentos e vantagens da criação de uma rede única da Defesa.

Considera-se que poderão decorrer futuras investigações que abordem os temas referidos no parágrafo anterior, bem como:

- Apoio que as TIC e a sua conjugação num centro conjunto, a centralização dos juristas adstritos à CD e a criação de uma única rede da Defesa poderiam dar à centralização dos CIRC;

- Requisitos técnicos necessários para a centralização dos CIRC;

- Estudo de uma IE (quer seja no *Campus* da Defesa quer seja noutro local) que possua os necessários requisitos (dimensionais, de segurança, etc.) que respondam às necessidades de deslocalização do CCD das atuais instalações, especialmente se se prosseguir para a centralização dos CIRC.

Bibliografia

Alexandre, C. (10 de outubro de 2019). *Entrevista presencial subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-16. (C. Pinho, Entrevistador) Almada, Portugal.

Aparício, M. d. (2017). *O Ciberespaço como Dimensão de Segurança*, i - 109. (Tese de Dissertação de Mestrado em Aeronáutica Militar). Academia da Força Aérea [AFA], Sintra. Retirado em 13 de setembro de 2019, de https://comum.rcaap.pt/bitstream/10400.26/23108/1/O%20ciberespa%C3%A7o%20como%20dimens%C3%A3o%20de%20seguran%C3%A7a_disserta%C3%A7%C3%A3o.pdf

Ashford, W. (2017, 06 de junho). Europe faces shortage of 350,000 cyber security professionals by 2022 [Página *online*]. Retirado em 10 de novembro de 2019, de https://www.computerweekly.com/news/450420193/Europe-faces-shortage-of-350000-cyber-security-professionals-by-2022

Bernardino, L. M. (2015, fevereiro). A Guerra Assimétrica a Segurança Marítima e a Cibersegurança. Perspetivas de Cooperação no espaço da CPLP. Em: Academia Militar, *Seminário Político-Diplomático do CAE/CPLP*. Seminário organizado pela Academia Militar, Lisboa. Retirado em 19 de setembro de 2019, de https://cplp.defesa.pt/CAE/VI%C2%BASeminarioPolitico-Diplom%C3%A1tico_TCor%20LuisBernardino_6Fev2015_VFinal.pdf

Carvalho, C. (04 de outubro de 2019). *Entrevista presencial subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-16. (C. Pinho, Entrevistador) Lisboa, Portugal.

Castro, A. (22 de novembro de 2019). *Entrevista presencial subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-14. (C. Pinho, Entrevistador) Lisboa, Portugal.

CEMGFA. (2018). *Diretiva Estratégica do Estado-Maior General das Forças Armadas*, 1 – 37 [versão PDF]. Lisboa, Portugal: EMGFA. Retirado em 15 de setembro de 2019, de https://www.emgfa.pt/documents/435jnqg1vmd7.pdf

CNCS. (2019a). Cidadão Ciberseguro [Página *online*]. Retirado em 15 de novembro de 2019, de CNCS: https://www.cncs.gov.pt/recursos/cidadao-ciberseguro/

CNCS. (2019b). *Quadro nacional de referência para a cibersegurança*, 1 - 171. Lisboa: Autor. Retirado em 08 de dezembro de 2019, de https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

Comissão, Europeia. (2016, 30 de novembro). Plano de ação europeu no domínio da defesa: para um fundo europeu de defesa, 1 – 4 [Notícia *online* – versão PDF]. Bruxelas: Comissão Europeia. Retirado em 13 de novembro de 2019, de https://ec.europa.eu/commission/presscorner/detail/pt/IP_16_4088

Conceito.de. (2011a). Conceito de eficácia [Página *online*]. Retirado em 04 de dezembro de 2019, de https://conceito.de/eficacia

Conceito.de. (2011b). Conceito de eficiência [Página *online*]. Retirado em 04 de dezembro de 2019, de https://conceito.de/eficiencia

Couto, A. C. (Org.). (1988). *Elementos de Estratégia* (Vol. I). Lisboa, Portugal: Instituto de Altos Estudos Militares. Retirado em 20 de novembro de 2019

Decreto-Lei n.º 184/2014, de 29 de dezembro (2014). *Aprova a Lei Orgânica do Estado-Maior General das Forças Armadas*. Diário da República, 1.ª Série, 250, 6382-6397. Lisboa: Governo. Retirado em 23 de setembro de 2019, de https://dre.pt/application/conteudo/65983261

Decreto Regulamentar n.º 13/2015, de 31 de julho (2015). *Aprova a orgânica do Estado-Maior-General das Forças Armadas*. Diário da República, 1.ª Série, 148, 5275 - 5295. Lisboa, Portugal: Governo. Retirado em 25 de setembro de 2019, de https://dre.pt/application/conteudo/69920325

Despacho n.º 13692/2013, de 11 de outubro (2013). *Orientação para a política de Ciberdefesa*. Diário da República, 2.ª Série, 208, 31976-31979. Lisboa: Ministério da Defesa Nacional. Retirado em 23 de setembro de 2019, de https://dre.pt/application/conteudo/3295679

Diretiva (UE) 2016/1148, de 06 de julho (2016). *Medidas Nível Comum Segurança Redes e Informação*. Jornal Oficial da União Europeia, 1 - 36. Estrasburgo: União Europeia. Retirado em 13 de novembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:194:FULL&from=PT

EMGFA. (2019a). *Relatório do Estudo de Desenvolvimento da Capacidade de Ciberdefesa*, 1 - E-5, (Relatório de Estudo). Lisboa, Portugal: Autor. Retirado em setembro de 2019

EMGFA. (2019b). *Plano de Desenvolvimento da Capacidade de Ciberdefesa*, 1 - B-3, (Plano). Lisboa, Portugal: Autor. Retirado em setembro de 2019

ENISA. (2016). *ENISA Strategy 2016-2020*, 1 - 16 [versão PDF]. Retirado em 13 de setembro de 2019, de https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Ferreira, L. M. (2018). *Gestão e sustentação de um quadro de pessoal especializado na área da ciberdefesa e da cibersegurança*, i - Apd F-9 (Trabalho de Investigação Individual – Curso de Estado Maior Conjunto). Instituto Universitário Militar [IUM], Pedrouços. Retirado em 31 de outubro de 2019, de https://comum.rcaap.pt/handle/10400.26/23208

Ferreira, R. R. (2019, 22 de fevereiro). Economia digital representa 4,6% do PIB português [Página *online*]. Retirado em 10 de novembro de 2019, de dinheirovivo.pt: https://www.dinheirovivo.pt/economia/economia-digital-representa-46-do-pib-portugues/)

Government, Heads of State and. (2010). *Active Engagement, Modern Defence* (Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization). Retirado em 28 de setembro de 2019, de https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

Governo. (2015, 08 de maio). Mercado Único Digital para a Europa: Comissão Europeia define 16 iniciativas para a sua concretização [Página *online*]. Retirado em 10 de novembro de 2019, de compete2020.gov.pt: https://www.compete2020.gov.pt/noticias/detalhe/Mercado-Unico-Digital-Europa

Governo. (2019, 24 de julho). Ministro da Defesa Nacional lança concurso de ideias para futuro Campus da Defesa [Página *online*]. Retirado em 17 de outubro de 2019, de https://www.portugal.gov.pt/pt/gc21/comunicacao/noticia?i=ministro-da-defesa-nacional-lanca-concurso-de-ideias-para-futuro-campus-da-defesa

Ideas, G., & Networks, A. (2015, 02 de janeiro). Digital Attack Map (DAM) [Página *online*]. Retirado em 12 de novembro de 2019, de https://www.digitalattackmap.com/

Ideas, G., & Networks, A. (2019, 12 de novembro). DAM [Página *online*]. Retirado em 12 de novembro de 2019, de https://www.digitalattackmap.com/

Jesus, F. d., & Assunção, C. d. (18 de novembro de 2019). *Entrevista subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-10. (C. Pinho, Entrevistador) Lisboa, Portugal.

Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring Corporate Strategy* (8 ed.). Essex, England: Pearson Education Limited. Retirado em 22 de dezembro de 2019, de https://epdf.pub/queue/exploring-corporate-strategy-8th-edition.html

Kobie, N. (2015, 6 de maio). What is the internet of things? [Página *online*]. Retirado em 25 de setembro de 2019, de the guardian: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google

Lei n.º 46/2018, de 13 de agosto (2018). *Estabelece o regime jurídico da segurança do ciberespaço*. Diário da República, 1.ª Série, 155, 4031 - 4037. Lisboa, Portugal: Assembleia da República. Retirado em 15 de outubro de 2019, de https://dre.pt/application/conteudo/116029384

Lei nº 109/2009, de 15 de setembro (2009). *Aprova a Lei do Cibercrime*. Diário da República, 1.ª Série, 179, 6319 - 6325. Lisboa, Portugal: Assembleia da República. Retirado em 15 de outubro de 2019, de https://dre.pt/application/conteudo/489693

Lei Orgânica nº 2/2019, de 19 de junho (2019). *Aprova a lei de programação militar e revoga a Lei Orgânica n.º 7/2015, de 18 de maio*. Diário da República, 1.ª Série, 114, 2982 - 2985. Lisboa, Portugal: Assembleia da República. Retirado em 15 de setembro de 2019, de https://dre.pt/application/conteudo/122592080

Lei Orgânica nº 7/2015, de 18 de maio (2015). *Aprova a lei de programação militar e revoga a Lei Orgânica n.º 4/2006, de 29 de agosto*, Diário da República, 1.ª Série, 95, 2554 - 2558. Lisboa, Portugal: Assembleia da República. Retirado em 15 de setembro de 2019, de https://dre.pt/application/conteudo/67232587

Lucas, A. & Silva, G. (2019). *Programa Prós e Contras – Quem protege a democracia?* [Programa de televisão]. Lisboa, Portugal: RTP1. Retirado em 03 de outubro de 2019, de https://www.rtp.pt/play/p5337/e401358/pros-contras

Lusa. (2019, 12 de novembro). Corbyn qualifica ataque cibernético ao Partido Trabalhista de "suspeito e preocupante" [Notícia *online*]. Retirado em 14 de novembro de 2019, de SIC Notícias: https://sicnoticias.pt/mundo/2019-11-12-Corbyn-qualifica-ataque-cibernetico-ao-Partido-Trabalhista-de-suspeito-e-preocupante

Marques, G. (08 de outubro de 2019). *Entrevista presencial subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-19. (C. Pinho, Entrevistador) Lisboa, Portugal.

Mateus, C. (2019, 23 de fevereiro). Afinal eles querem um emprego para a vida [Notícia *online*]. Retirado em 07 de novembro de 2019, de Expresso: https://expresso.pt/economia/2019-02-23-Afinal--eles-querem--um-emprego-para-a-vida

MDN. (2014). *Conceito Estratégico Militar*, i - 45. Lisboa, Portugal.

MDN. (2019). *Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa* (Despacho nº 52/MDN/2019). Lisboa, Portugal: Autor. Retirado em 02 de novembro de 2019

NATO. (2016). *Performance audit report to Council on the need to improve NATO's*, 1-45 (IBA-AR(2016)05). Bruxelas, Bélgica: International Board of Auditors for NATO. Retirado em 28 de dezembro de 2019, de https://www.nato.int/issues/iban/performance_audits/170201-improve-capability-package-process-eng.pdf

NATO. (2017, fevereiro). Warsaw Summit Key Decisions [*Fact Sheet*]. Retirado em 26 de setembro de 2019, de https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

NATO. (2018). *High Level Taxonomy of Cyberspace Operations*, 1 - A-2-7. (IMSM-0222-2018) Norfolk, Virgínia, EUA: Headquarters Supreme Allied Commander Transformation. Retirado em 09 de janeiro de 2020, de https://webmail.marinha.pt/owa/#viewmodel=ReadMessageItem&ItemID=AAMkAGZmMzRhYWJmLWY4ZmEtNDFlYy05YWRhLTVkZWQ5YjlmMDBlMgBGAAAAAAAkv6%2B0qhNlR5OBvnSp27VjBwCOFERPXUQ6SLkOqSZ%2FWCA8AAMx8osoAACOFERPXUQ6SLkOqSZ%2FWCA8AAOFMHzzAAA%3D&wid=86&ispopout=1

NATO. (2019, 04 de dezembro). London Declaration [Notícia *online*]. Londres, Reino Unido. Retirado em 10 de dezembro de 2019, de https://www.nato.int/cps/en/natohq/official_texts_171584.htm?selectedLocale=en

NATO. (11 de novembro de 2019). *AAP-06 NATO Glossary of terms and definitions*. Brussels, Bélgica: NATO Standardization Office. Obtido em 04 de dezembro de 2019, de https://standard.di.mod.bg/pls/mstd/MSTD.blob_upload_download_routines.download_blob?p_id=281&p_table_name=d_ref_documents&p_file_name_column_nam

e=file_name&p_mime_type_column_name=mime_type&p_blob_column_name=contents&p_app_id=600

NCIA. (2020). *Indicative C4ISR and Cyber Training Catalogue Price List*, 1 – 8 [versão PDF]. NCIA. Retirado em 10 de janeiro de 2020, de https://www.ncia.nato.int/SiteCollectionDocuments/Course%20pricing%20model%202020%20v4%20edit%20CMC.pdf

Neves, P. J. (2015). *Capacidade de Resposta a Incidentes de Segurança da Informação no Ciberespaço uma abordagem DOTMLPI-I,* 1 - 123. (Tese de Dissertação de Mestrado em Segurança da Informação e Direito no Ciberespaço). Escola Naval [EN], Almada, Instituto Superior Técnico, Lisboa, Faculdade de Direito da Universidade de Lisboa, Lisboa, Portugal. Retirado em 01 de novembro de 2019, de https://fenix.tecnico.ulisboa.pt/downloadFile/1126295043834849/MestradoSIDC(PNeves).pdf

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, i – 48 [versão PDF]. Retirado em 24 de setembro de 2019, de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nunes, P. F. (2012). *A Definição de uma Estratégia Nacional de Cibersegurança*, 1 - 259. [versão PDF]. Lisboa, Portugal: Instituto da Defesa Nacional. Retirado em 31 de outubro de 2019, de https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf

Nunes, P. V., Mendes, C. P., Ralo, J., Santos, L., Santos, L. C., Moniz, P., & Casimiro, S. d. (2018). *Contributos para uma Estratégia Nacional de Ciberdefesa, 28*, 1 – 102 [versão PDF]. Lisboa, Portugal: IDN. Retirado em 14 de setembro de 2019, de https://www.idn.gov.pt/publicacoes/cadernos/idncadernos_28.pdf

Pinto, J. (2019, 11 de setembro). Ciber-ataques causam perdas com o valor mais elevado de sempre [Notícia *online*]. Retirado em 10 de novembro de 2019, de noticias e tecnologia: https://noticiasetecnologia.com/ciber-ataques-perdas-valor-elevado-sempre/

Rego, A., Cunha, M., & Meyer, V. (2018). Quantos participantes são necessários para um estudo qualitativo?. Revista de GESTÃO dos Países de Língua Portuguesa, pp. 1-15.

Regulamento (UE) 2016/679, de 27 de abril de 2016a). *Regulamento Geral sobre a Proteção de Dados*, Jornal Oficial da União Europeia, L 119/1 - L 119/88. Bruxelas: Comissão

Europeia. Retirado em 02 de novembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT

Regulamento (UE) 2019/881, de 17 de abril de 2019). *Certificação da Cibersegurança das tecnologias da informação e comunicação*, Jornal Oficial da União Europeia, L 151/15 - L 151/69. Estrasburgo: Comissão Europeia. Retirado em 25 de setembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881&from=PT

Regulamento de Execucão (UE) 2018/151, de 30 de janeiro de 2018). *Normas Execucão Segurança Redes e Sistemas Informação, Jornal Oficial da União Europeia*, L 26/48 - L26/51. Bruxelas: Comissão Europeia. Retirado em 13 de novembro de 2019, de https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF/?uri=CELEX:32018R0151&from=PT

Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro (2015a). *Estratégia Nacional de Combate ao Terrorismo*. Diário da República, 1.ª Série, 36, 1022-(2) - 1022-(4). Lisboa: Assembleia da República. Retirado em 15 de outubro de 2019, de https://dre.pt/application/conteudo/66567251

Resolução do Conselho de Ministros nº 19/2013, de 05 de abril (2013a). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª Série, 67, 1981 - 1995. Lisboa, Portugal: Assembleia da República. Retirado em 14 de setembro de 2019, de https://dre.pt/application/conteudo/259967

Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril (2013b). *Reforma «Defesa 2020»*. Diário da República, 1.ª Séria, 77, 2285 - 2289. Lisboa, Portugal: Assembleia da República. Retirado em 25 de setembro de 2019, de https://dre.pt/application/conteudo/260395

Resolução do Conselho de Ministros nº 36/2015, de 28 de maio (2015b). *Aprova a Estratégia Nacional de Segurança do Ciberespaço*. Diário da República, 1.ª Série, 113, 3738 - 3742. Lisboa, Portugal: Assembleia da República. Retirado em 14 de setembro de 2019, de https://dre.pt/application/conteudo/67468089

Resolução do Conselho de Ministros n.º 41/2018, de 28 de março (2018). *Regime de Proteção de Dados Pessoais*. Diário da República, 1.ª Série, 62, 1424 - 1430. Lisboa: Assembleia da República. Retirado em 14 de outubro de 2019, de https://dre.pt/application/conteudo/114937034

Resolução do Conselho de Ministros nº 92/2019, de 05 de junho (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1.ª Série, 108, 2888 - 2895. Lisboa, Portugal: Assembleia da República. Retirado em 31 de outubro de 2019, de https://dre.pt/application/conteudo/122498962

Ribeiro, A. A. (2009). *Teoria Geral da Estratégia: o essencial ao processo estratégico.* (Vol. vol. I). Coimbra: Edições Almedina, SA. Retirado em 15 de dezembro de 2019

RNCSIRT. (2019). Rede Nacional CSIRT [Página *online*]. Retirado em 16 de novembro de 2019, de Rede CSIRT: https://www.redecsirt.pt/

Rosa, Q. (08 de novembro de 2019). *Entrevista presencial subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-31. (C. Pinho, Entrevistador) Lisboa, Portugal.

SANS. (2020). OnDemand: Courses & Prices [Página *online*]. Retirado em 10 de janeiro de 2020, de SANS: https://www.sans.org/ondemand/courses/all/

Santos, L. (2016). A Internet de Tudo [Artigo *online*]. Retirado em 14 de novembro de 2019, de LinkedIn: https://pt.linkedin.com/pulse/internet-de-tudo-leonardo-santos

Santos, L., Lima, J., Garcia, F., Monteiro, F., Silva, N., Silva, J., . . . Piedade, J. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação.* (I. -C. Desenvolvimento, Ed.) Pedrouços: Instituto Universitário Militar. Retirado em 29 de setembro de 2019, de https://sites.ium.pt/moodle/course/view.php?id=186

Teixeira, J. (08 de janeiro de 2020). *Entrevista subordinada ao tema "O modelo de ciberdefesa nacional. Solução centralizada ou distribuída?"*, 1-8. (C. Pinho, Entrevistador)

US, J. C. (2018). *JP 3-12 Cyberspace Operations*, 1 - IV-26 [versão PDF]. United States. Retirado em 25 de setembro de 2019, de https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

wearesocial. (2015). Digital, Social & Mobile Worldwide in 2015 [Página *online*]. Retirado em 20 de setembro de 2019, de https://wearesocial.com/uk/special-reports/digital-social-mobile-worldwide-2015

wearesocial. (2019). Digital, Social & Mobile Worldwide in 2019 [Página *online*]. Obtido em 20 de setembro de 2019, de https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

WEF. (2016). The Global Risks Report 2015 [Página *online*]. Retirado em 20 de setembro de 2019, de http://reports.weforum.org/global-risks-2015/executive-summary/

WEF. (2019). *The Global Risks Report 2019* [versão PDF]. Retirado em 20 de setembro de 2019, de http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

weforum. (2016). *We Forum Reports – Portuguese* [versão PDF]. Retirado em 20 de setembro de 2019, de weforum: http://reports.weforum.org/global-risks-2015/wp-content/blogs.dir/68/mp/files/pages/files/grr15-executivesummary-portuguese.pdf

Anexo A - Corpo de Conceitos

Tabela 1 – Corpo de Conceitos

Capacidade – "*The ability to create an effect through employment of an integrated set of aspects categorized as doctrine, organization, training, materiel, leadership development, personnel, facilities, and interoperability*" (NATO, 2019, p. 23).
CD – "Atividade que visa assegurar a defesa nacional no ou através do ciberespaço" (RCM 92/2019, 2019, p. 2889).
Ciberespaço – "Ambiente complexo de valores e interesses materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas e redes e sistemas de informação" (RCM 92/2019, 2019, p. 2889).
CS – "Conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem" (RCM 92/2019, 2019, p. 2889).
CSIRT – "equipa que atua por referência a uma comunidade de utilizadores definida, em representação de uma entidade, prestando um conjunto de serviços de segurança que inclua, designadamente, o serviço de tratamento e resposta a incidentes de segurança das redes e dos sistemas de informação" (L 46/2018, 2018, p. 4031).
Doutrina – "Numa perspetiva militar, a Doutrina aparece ligada ao modo como são conduzidas as operações de combate, sejam as manobras ou as campanhas, ou seja, os princípios fundamentais que permitem a utilização coordenada de uma ou mais forças militares para atingir um objetivo comum. A Doutrina baseia-se os princípios comuns construídos sobre as lições aprendidas durante as operações militares, através de treinos e exercícios. Considerando a sua caraterística imperativa para as Forças militares em campanha, esta está sempre sujeita às políticas comuns acordadas entre as partes, aos tratados e a restrições de natureza legal, devendo ser sempre seguida, exceto se, de forma muito excecional, o comandante em exercício assim o entender" (Neves, 2015, p. 51).
Eficácia – "Do latim *efficacĭa*, a eficácia é a capacidade de alcançar o efeito esperado ou desejado através da realização de uma ação" (Conceito.de, 2011a).
Eficiência – "A palavra eficiência tem origem no termo latim *efficientĭa* e refere-se à capacidade de dispor de alguém ou de algo para conseguir um efeito determinado. O conceito também costuma ser equiparado com o de acção, força ou produção" "Uso racional dos meios dos quais se dispõe para alcançar um objetivo previamente determinado. Trata-se da capacidade de alcançar os objetivos e as metas programadas com o mínimo de recursos disponíveis e tempo, conseguindo desta forma a sua otimização" (Conceito.de, 2011b).
Estratégia (Perspetiva) Genética – "tem por objecto a invenção, construção ou obtenção de novos meios a colocar à disposição da estratégia operacional, no momento adequado, e que servem o conceito estratégico adoptado e tenham em atenção a evolução previsível da conjuntura" (Couto, 1988, p. 231).
Estratégia (Perspetiva) Estrutural – "tem por objectivo a detecção e análise das vulnerabilidades (ou pontos fracos) e das potencialidades das estruturas existentes, com vista à definição das medidas mais adequadas, incluindo a criação de novas estruturas, que conduzam à eliminação ou atenuação das vulnerabilidades, a um reforço das potencialidades e, em última análise, a um melhor rendimento dos meios ou recursos" (Couto, 1988, p. 232).
Estratégia (Perspetiva) Operacional – "pôr em prática as acções específicas de emprego dos meios para alcançar os objectivos. O seu objecto é, não só, conciliar os objectivos a atingir com as possibilidades proporcionadas pelas estratégias genética e estrutural, mas, também, orientar a evolução destas, de forma a adaptá-las às necessidades operacionais" (Ribeiro, 2009, p. 33).
Fator Ambiental – "*stands specifically for 'green' issues, such as pollution and waste*" (Johnson, Scholes, & Whittington, 2008, p. 55).
Fator Económico – "*refers to macro-economic factors such as exchange rates, business cycles and differential economic growth rates around the world*" (Johnson, Scholes, & Whittington, 2008, p. 55).
Fator Legal – "*embraces legislative constraints or changes*" (Johnson, Scholes, & Whittington, 2008, p. 55).
Fator Político – "*highlights the role of governments*" (Johnson, Scholes, & Whittington, 2008, p. 55).
Fator Sociocultural – "*include changing cultures and demographics*" (Johnson, Scholes, & Whittington, 2008, p. 55).
Fator Tecnológico – "*refer to innovations such as the Internet, nanotechnology or the rise of new composite materials*" (Johnson, Scholes, & Whittington, 2008, p. 55).

Infraestrutura crítica – "componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem -estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções" (L 46/2018, 2018).
Infraestruturas – "são tudo o que se refere com a disponibilização de instalações adequadas à preparação e condução das operações. Também aqui é importante garantir que as Infraestruturas existentes permitem responder de forma satisfatória aos requisitos de manutenção em tempo de paz e aos requisitos operacionais em tempo de crise. Estas poderão variar de acordo com as necessidades da missão, mas de uma forma geral estamos a falar de edifícios administrativos, oficinas, armazéns, centros de dados, estradas, distribuição de energia elétrica e água, entre outras" (Neves, 2015, p. 53).
Interoperabilidade – "O estabelecimento desta abordagem comum implica que se utilize um conjunto de conceitos partilhados entre as partes, que todos entendam como válidos. Isto pode ser conseguido através de políticas que definam procedimentos similares que sejam facilitadores de uma verdadeira interoperabilidade entre equipas pertencentes a estruturas organizacionais diferentes, mas que colaboram para o atingir do mesmo objetivo" (Neves, 2015, p. 53).
IoE – ligação de "pessoas**,** processos, dados e coisas" (quatro pilares da IoE) "para fazer conexões de rede mais relevante e valioso do que nunca, transformando as informações em ações que criam novas capacidades, experiências mais ricas e oportunidade económica sem precedentes para as empresas, indivíduos e países" (Santos L. , 2016).
IoT – "*a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices*" "IoT *is more than smart homes and connected appliances, however. It scales up to include smart cities*" (Kobie, 2015).
Liderança – "surge diretamente ligada à Formação, preocupando-se essencialmente com a preparação das chefias para uma abordagem profissional da operação, ou seja ao desenvolvimento da competência profissional para comandar. É fundamental que o líder seja capaz de compreender o objetivo que lhe é apresentado e que conduza a ação para que este seja alcançado com sucesso. Tem de ter a capacidade de dirigir e motivar os membros da equipa, com profissionalismo, sabendo aproveitar eficazmente as mais-valias dos vários elementos, consolidando ou mesmo desenvolvendo as suas capacidades com vista ao sucesso da missão" (Neves, 2015, p. 52).
Material – "refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais. Esta dimensão abrange desde os equipamentos, à tecnologia, às armas, ou as infraestruturas de comunicações, ou seja, todo o material que tenha relevância para o sucesso da missão. Os problemas que surgem nesta área podem ter soluções de natureza material, adquirindo o artigo necessário para a sua resolução. Por outro lado também podem ser problemas que não sejam resolúveis através de qualquer aquisição, ou seja, terão de ter uma solução não-material, implicando assim soluções que envolvam alterações nas outras dimensões, como por exemplo na doutrina, na organização ou no treino" (Neves, 2015, p. 52).
Organização – "diz respeito ao modo como os indivíduos se constituem como equipas, e estas em unidades operacionais, executando as funções que lhes são determinadas, de forma a contribuírem para o sucesso da missão. Estas unidades operacionais são suportadas numa estrutura que permite que funcionem de forma coordenada" (Neves, 2015, p. 51).
Pessoal – "o mais importante é garantir que este possui as qualificações necessárias para o desempenho da missão, quer considerando as necessidades em tempo de paz, quer em tempo de crise. O fator humano e a componente social são determinantes, competindo à estrutura de comando a responsabilidade de identificar os elementos mais capazes para o desempenho das tarefas e disponibilizarem-lhes a formação adequada. Por outro lado, é preciso considerar que para algumas missões, o pessoal pode não ter as competências necessárias, sendo por isso necessário envolver pessoal externo ou parceiros civis, como sejam as empresas do setor tecnológico ou outras, para que se possa cumprir a missão. Quando identificadas lacunas na formação do nosso pessoal, ou o surgimento da necessidade de novas competências relevantes para a missão, deve ser feita a ponderação de alteração do plano de formação previsto para os diferentes papéis que os elementos desempenham no seio da equipa ou a contratualização do serviço a entidades externas. Finalmente há que considerar um quadro de pessoal que garanta a disponibilidade dos recursos humanos necessários quer em tempo de paz quer em tempo de crise" (Neves, 2015, p. 53).
Serviço essencial – "um serviço essencial para a manutenção de atividades societais ou económicas cruciais, que dependa de redes e sistemas de informação e em relação ao qual a ocorrência de um incidente possa ter efeitos perturbadores relevantes na prestação desse serviço" (L 46/2018, 2018).
Treino – "Treino das equipas é fundamental, sejam estas operacionais ou de suporte às várias estruturas que participam nas operações, sejam unidades individuais, de grupo ou mesmo alianças internacionais. (…) As lições aprendidas através do treino permitem a revisão ou mesmo o desenvolvimento de novos conceitos com impacto direto no aperfeiçoamento das capacidades operacionais" (Neves, 2015, p. 52).

Apêndice A — Análise do ambiente externo

Tabela 2 – Análise PESTAL

Fator Político – Esta análise política incidirá em duas vertentes distintas, uma vertente internacional e uma vertente nacional que não estarão intrinsecamente separadas.

Decorrente dos incidentes nos Balcãs no final dos anos 90, no seio da NATO, oficializado na cimeira de Praga em 2002, que a NATO começa o seu programa de CD sendo criado após a cimeira de Istambul em 2004 o NATO CIRC para dar resposta a ciberataques. Na cimeira de Bucareste em 2008, é emanada a Primeira Política de CD da NATO (Aparício, 2017) (Ferreira L. M., 2018).

Em 2010 na cimeira de Lisboa, é aprovado no âmbito NATO um novo Conceito Estratégico (CE) onde é defendido a noção de "Abordagem Global" (*Comprehensive Approach*), articulando meios militares e civis na resposta a desafios no âmbito da CD e CS, face às falhas identificadas na NATO e pelos seus Estados Membros (RCM 19/2013, 2013a) (Aparício, 2017, p. 56).

Em 2011 os Ministros da Defesa dos Estados Membros da NATO assinaram a Segunda Política de CD e em 2013 foi apresentada a Estratégia de CS da UE definindo cinco prioridades estratégicas (Aparício, 2017).

Em 2014, decorrente da Cimeira de Gales, a NATO, mas também a UE apresentam as suas *Cyber Defence Policy* identificando áreas prioritárias da CD e em 2016 foi elaborado um acordo técnico entre a NATO e a UE para partilha de informações, melhores práticas e ações (Aparício, 2017).

Ainda em 2016, na cimeira de Varsóvia, talvez se dê a transformação política que influencia determinantemente a atuação nacional e internacional no âmbito do ciberespaço, sendo usado pelos mais diversos atores, estatais e não estatais, exercendo através dele poder no "domínio social, político/diplomático, económico e até militar" reconhecendo-o como 4º Domínio Operacional, "associando este novo espaço de condução de operações militares ao ambiente terrestre, naval e aéreo" (Nunes, et al., 2018, p. 11).

Também se denota a preocupação de diversos países aliados com a CD, através de financiamento reforçado nesta matéria, bem como da elevação da importância dada a quem lida com estas matérias, através da criação de Comandos Cibernéticos, como por exemplo nos EUA, ou mesmo através da criação de um ramo das FFAA (Alemanha). (EMGFA, 2019a).

A nível nacional, desde 2013 que se denota a crescente importância dada ao ciberespaço, desde logo no CEDN, quer a nível da CS quer a nível da CD atribuindo às FFAA o "maior grau de prioridade (…) ao desenvolvimento da capacidade de ciberdefesa" (RCM 19/2013, 2013a, p. 1992) bem como através da "Orientação para a política de Ciberdefesa" (DESPACHO 13692/2013, 2013, p. 31977). Ainda em 2013 é emanada uma reforma estrutural denominada "Defesa 2020" que "responde ao desafio da mudança" visando "obter ganhos de eficiência, economias de escala" através do princípio da concentração de recursos através de capacidades militares integradas (RCM 26/2013, 2013b, p. 2285).

A Resolução do Conselho de Ministros (RCM) nº 36/2015 aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) (RCM 36/2015, 2015b, pp. 3739-3740) revogada pela RCM nº 92/2019 que aprovou a ENSC 2019-2023, que "assenta em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos" e nos princípios da subsidiariedade, complementaridade e proporcionalidade (RCM 92/2019, 2019, pp. 2889-2890).

Está a ser desenvolvido um documento orientador em CD, a ENCD, que "estará em alinhamento com a ENCS 2019-2023", tendo terminado em setembro de 2019 o desenvolvimento dos "princípios orientadores para a mesma (Marques, 2019) (Despacho nº 52/MDN/2019, 2019).

Fator Económico - Estando atualmente cada vez mais a viver-se na Era da Informação, esta realidade tem implicações em diversos setores, nomeadamente no setor económico, no qual, cada vez mais esta Era é "caracterizada pela existência de uma economia cada vez mais centrada em rede". Portugal, acompanhando a tendência mundial, tem-se tornado cada vez mais dependente da internet e das TIC pelo que a "utilização maliciosa do ciberespaço pode ter por alvo indivíduos, organizações ou até Estados, afetando os processos de geração de riqueza" (Nunes, et al., 2018, p. 13).

No Plano de Ação Europeu no Domínio da Defesa, a Comissão Europeia salienta diversos aspetos importantes, como o facto de "ao longo da última década, os Estados-Membros da UE diminuíram os seus gastos com a defesa em cerca de 12% (…) enquanto outros importantes intervenientes globais (China, Rússia e Arábia Saudita) têm vindo a reforçar o respetivo setor da defesa numa escala sem precedentes. Em 2015, os EUA investiram na defesa mais do dobro da despesa total dos Estados-Membros da UE. A China aumentou o seu orçamento de defesa em 150 % ao longo da última década." Como razões para o investimento na defesa, é referido que "a ausência de cooperação entre os Estados-Membros no domínio da defesa e da segurança custe anualmente entre 25 000 milhões e 100 000 milhões" de euros e que "cada euro investido na defesa gera um retorno de 1,6" (Comissão, Europeia, 2016, pp. 2-3).

A crescente importância dada em Portugal à CD é patente no incremento orçamental alocado na LPM que teve um incremento de 14 milhões de euros de 2015-2026 para 45,5 milhões de euros 2019-2030 (2015) (2019). Este investimento poderá ser justificado pelo crescente peso da economia digital em Portugal. Em 2017 contribuiu com o equivalente a 4,6% do PIB (nove mil milhões de euros), podendo este valor ascender a mais de 20 mil milhões de euros já em 2025 (Ferreira R. R., 2019).

A UE define, para a concretização do Mercado Único Digital para a Europa, uma estratégia assente em três pilares: "1) Melhor acesso dos consumidores e empresas a bens e serviços digitais em toda a Europa, 2) Criação de condições adequadas e de condições de concorrência equitativas para o desenvolvimento de redes digitais e de serviços inovadores, 3) Otimização do potencial de crescimento da economia digital."

Propõe igualmente diversas ações-chave assentes em três pilares: "Melhor acesso dos consumidores e empresas aos bens e serviços digitais em toda a Europa", "Criação de condições adequadas e de condições de concorrência equitativas para o desenvolvimento de redes digitais e serviços inovadores" e "Otimização do potencial de crescimento da economia digital". É ainda referido que "um Mercado Único Digital plenamente funcional poderia contribuir com 415 mil milhões de euros por ano para a nossa economia e criar centenas de milhares de novos postos de trabalho" (Governo, 2015).

Crescendo a economia digital, como é natural, também se estima que haja um aumento das perdas decorrentes de ataques cibernéticos, para um valor global de 6 triliões de euros até 2021 (Pinto, 2019).

Fator Sociocultural – O desenvolvimento económico explanado anteriormente, faz com que muitas empresas necessitem de aumentar em cerca de 15% a sua equipa de CS o que faz com que se preveja uma falta de 350000 RH nesta área de especialidade (Ashford, 2017). Também em Portugal atualmente se sente a falta de 15000 especialistas em CS (Marques, 2019).

É notório o grande aumento de utilizadores de Internet e das redes sociais, fruto da "Era Digital". Em apenas 4 anos houve um crescimento acentuado dos utilizadores de internet (45,78%) mas o crescimento mais notório foi nos utilizadores de redes sociais através do telemóvel (93,23%).

Estes números explicam a crescente preocupação global com os ciberataques e com o acesso a IE criticas.

Com a denominada geração dos *millennials*, profissionais dispostos a arriscar e com uma visão de carreira disruptiva, que dão uma menor relevância a um "emprego para a vida" começou a colocar-se a problemática da retenção de RH com oportunidades de emprego bastante aliciantes no mundo civil. Esta tendência poderá reverter com a chegada ao mercado de trabalho da "geração Z", uma geração que cresceu com a crise e com a "recessão global, que viu os pais perderem o emprego, que viveu momentos de grande instabilidade e insegurança. (…) No que toca ao emprego esta geração quer "segurança, planos de carreira e um escritório físico para trabalhar". Por outras palavras, enquanto os *millennials* estavam formatados para mudar de emprego a cada dois anos, os profissionais da geração Z permanecerão na mesma empresa toda a vida, desde que esta garanta um processo atrativo de progressão e formação e um ambiente de trabalho inclusivo" (Mateus, 2019).

Como uma das grandes ameaças para os Estados democráticos e para as entidades políticas, fruto que o "processo de globalização e a revolução tecnológica tornaram possível (...) uma difusão (...) de ameaças e riscos em todas as dimensões, que incluem tanto a projeção das redes terroristas e de crime organizado, como a proliferação das armas de destruição massiva, a fragilização de Estados e o potencial devastador dos ataques cibernéticos" (RCM 19/2013, 2013a, p. 1983), começando o ciberespaço a ser utilizado, não só para facilitar "o acesso livre e aberto ao conhecimento e informação, agilizando a criação de movimentos, a partilha de ideologias e mesmo potenciando revoluções – como exemplo a revolução na Tunísia onde a internet foi a plataforma de convocação para um objetivo político comum" (Nunes, et al., 2018, p. 20) agindo o ciberespaço como uma rede única, com motivações diversas e riscos que é necessário acautelar e gerir, devido ao facto da informação viajar "de forma instantânea por todo o globo, e as tecnologias emergentes aumentaram muito a influência dos novos jogadores e novos tipos de guerra" (weforum, 2016).

Fator Tecnológico – Tem-se denotado uma acentuada evolução tecnológica bem como o "rápido crescimento da Internet", assumindo-se como "uma incontornável ferramenta de comunicação e interação à escala planetária, construíram uma "sociedade em rede" de matriz digital", evidenciando o facto de o ciberespaço não ser "limitado pela esfera pública ou privada, civil ou militar, interna ou externa" (Nunes, et al., 2018, p. 11).

Começou-se então a falar na denominada IoT. Posteriormente, uma vez que cada dispositivo passou a ser concebido com base num identificador único e com o pré-requisito de ligação a esta rede global, o mundo passou a estar permanentemente *on-line*, aprofundando uma cultura de partilha e conectividade, a que hoje atribuímos a designação de IoE, assumindo que o pilar "coisas" é o correspondente à IoT (Santos L. , 2016).

Verifica-se que através do ciberespaço consegue-se, a baixos custos obter consequências bastante elevadas, tendo por alvos de ações maliciosas, "indivíduos, organizações ou até Estados, afetando os processos de geração de riqueza e a construção plena de uma cidadania digital, condicionando o exercício dos direitos, liberdades e garantias" (Nunes, et al., 2018, p. 13).

Deste modo, torna-se necessário sensibilizar e educar, tendo o CNCS o curso "Cidadão Ciberseguro" que visa dar "conhecimentos sobre a vertente comportamental da segurança da informação, como forma de proteger os cidadãos dos incidentes de cibersegurança" (CNCS, 2019a).

Além dos cidadãos, individualmente, existe colaboração com a indústria nacional e com outros órgãos do Estado, que neste momento se encontra a ser efetuada primariamente pelo CNCS, existe o planeamento civil de emergência do ciberespaço ("previsto no sistema nacional de planeamento civil de emergência, sob coordenação da ANPC"[19]) (EMGFA, 2019a, pp. B-11).

Além da colaboração interna, de modo a "contribuir para o desenvolvimento da confiança entre os Estados-Membros e promover uma cooperação operacional célere e eficaz", bem como "alcançar um nível elevado de segurança das redes e dos sistemas de informação", foi criada a Rede Europeia de CSIRT's (Diretiva (UE) 2016/1148, 2016b, p. 7 e 13). A UE emitiu o regulamento para a "gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação" (Regulamento de Execucão (UE) 2018/151, 2018, p. L 26/48), bem como um regulamento relativo à "certificação da cibersegurança das" TIC (Regulamento (UE) 2019/881, 2019) e a NIST elabora em 2018 o "*Framework for Improving Critical Infrastructure Cybersecurity*" (NIST, 2018, p. i).

Fator Ambiental – O ambiente de segurança global confronta-se com diversos riscos e ameaças, nomeadamente o "ciberterrorismo e a cibercriminalidade, tendo por alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada" (RCM 19/2013, 2013a, p. 1984), reforçando "que o ambiente mundial se tornou mais incerto e menos seguro" (Regulamento (UE) 2019/881, 2019, p. L 151/18) tendo o ambiente cibernético algumas características próprias, tais como: "caráter dinâmico, baixo custo de acesso, enorme potencial de crescimento, alta capacidade de processamento de informação, caráter assimétrico, anonimato, alta capacidade para produzir efeitos físicos, transversalidade dos seus impactos" (Bernardino, 2015, p. 17).

Este ambiente favorece ataques e/ou distúrbios ao normal funcionamento dos Estados, tais como o da Estónia em 2007, da Geórgia em 2008, do Irão em 2009, na Ucrânia em 2014 (Nunes, et al., 2018) e a partidos políticos como ao Partido Trabalhista britânico em 2019 (Lusa, 2019) estando estes ataques "a tornar-se mais frequentes e organizados, ameaçando não só a segurança e estabilidade, como a prosperidade de cada Estado" (Aparício, 2017, p. 2) utilizando o ciberespaço para uma guerra híbrida "tirando partido das oportunidades nele criadas, (…) que permite transformá-lo numa ferramenta de propaganda, manipulação e distorção da informação", "através da sua utilização enquanto domínio operacional utilizado para o combate, de modo a complementar ou amplificar os efeitos das operações militares convencionais" sendo o combate à guerra híbrida conduzido e assente no princípio da indivisibilidade da segurança, significando que "todos os aliados deverão ser capazes de responder homogeneamente a ataques dirigidos contra qualquer ponto situado na área de responsabilidade da NATO" (Nunes, et al., 2018, pp. 33-34) o que, pode-se mesmo dizer que torna necessário a aquisição de uma "cultura de cibersegurança" (Nunes, et al., 2018, p. 11) e a consciencialização coletiva de modo a promover "esforços para que as FFAA dos seus Estados-membros possuam uma capacidade para intervir no domínio cibernético de forma a assegurar, em situações de exceção, o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado" (EMGFA, 2019a, pp. B-16) (ENISA, 2016).

Quando falamos em instituições que podem colocar em causa o regular funcionamento do exercício das normais funções e mesmo das funções de soberania do Estado, ou que têm "grande impacto económico-financeiro", falamos em instituições ou IE críticas, que em Portugal estão identificadas algumas tais como a Rede de Transportes, Sistema Financeiro, Sistema de Defesa (radares e mísseis), Proteção Civil (bombeiros), Sistema de Saúde, Sistema de Distribuição de Água, Rede de Telecomunicações e Rede Elétrica Nacional (Aparício, 2017, p. 47).

Fator Legal – Sendo o ciberespaço caracterizado por ser um "espaço aberto desprovido de fronteiras tangíveis", é imprescindível promover a cooperação entre Estados e no seio de organizações internacionais (DESPACHO 13692/2013, 2013, p. 31977).

Desde 2014 que a NATO reconhece a "aplicabilidade do Direito Internacional no ciberespaço", sendo as operações militares reguladas pelo mesmo, incluindo o Direito Internacional Humanitário. Reconhece igualmente que um ciberataque pode ser considerado "de acordo com a Carta das Nações Unidas (Artigo 51º)," e que no caso do Estado atacado pertencer à NATO poder invocar o "Artigo 5º do Tratado de Washington" (Nunes, et al., 2018, p. 40).

[19] Autoridade Nacional de Proteção Civil

Ainda no âmbito NATO, em 2013 o CCDCOE elaborou a primeira edição o Manual de Tallinn[20] tendo sido reeditada em 2017. Este manual procura, "uma vez que as normas internacionais que compõem o Direito Internacional dos Conflitos e o Direito Internacional Humanitário resultam de um longo e demorado processo, assente essencialmente no costume," "acelerar esse processo, apontando respostas para questões jurídicas que, num contexto como o do ciberespaço, não se compadecem com demoras" no âmbito da condução de operações no ciberespaço (Nunes, et al., 2018, p. 51).

No âmbito da UE foi efetuada em 2001 a Convenção sobre o Cibercrime e, entre outras iniciativas, o regulamento "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (Regulamento (UE) 2016/679, 2016a, p. L 119/1).

Em Portugal existem diplomas aplicáveis ao cibercrime, tais como a "Lei do Cibercrime" (Lei nº 109/2009, 2009, p. 6319) , a "Estratégia Nacional de Combate ao Terrorismo" (RCM 7-A/2015, 2015a, pp. 1022-(2)), o "regime jurídico da segurança do ciberespaço" (transpondo a Diretiva (UE) 2016/1148) (L 46/2018, 2018, p. 4031) e o "regime em matéria de proteção de dados pessoais" (derivado do Regulamento (UE) 2016/679) (RCM 41/2018, 2018, p. 1424).

Foram também emitidas a nível nacional diversas estratégias enquadrando, entre outras matérias, a atuação no ciberespaço, tais como o CEDN de 2013 (RCM 19/2013, 2013a), a ENSC de 2015 e de 2019 (RCM 36/2015, 2015b) (RCM 92/2019, 2019), e o Conceito Estratégico Militar de 2014 (MDN, 2014). A *European Union Agency for Network and Information Security* (ENISA) *strategy* 2016-2020 (ENISA, 2016) a nível da UE e a nível da NATO por exemplo o "*Strategic Concept for the Defence and Security of the Member of the*" NATO de 2010 (Government, Heads of State and, 2010).

Apesar destes diplomas legais, "num Estado de Direito, a segurança e a defesa têm de atuar num quadro legal bem definido" existindo ainda muitas zonas cinzentas sendo necessário continuar a adaptar o quadro legal ao "crescente protagonismo deste novo domínio" pois as "questões jurídicas suscitadas pelo ciberespaço são inúmeras e tendem a crescer à medida que as potencialidades das novas TIC se expandem" pois estas irão estar sempre a mudar, a um ritmo eventualmente maior que a capacidade de resposta do Direito (EMGFA, 2019a, pp. B-19).

[20] Conhecido abreviadamente como Manual de Tallinn, tem como título completo da 1ª edição, de 2013, *Tallinn Manual on the International Law Applicable to Cyber Warfare* e na 2ª edição, de 2017 o nome *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* consistindo num trabalho de especialistas em Direito Internacional dos Conflitos e em Direito Internacional Humanitário.

Apêndice B — Síntese da análise das entrevistas

Tabela 3 – Resumo entrevista CALM Gameiro Marques – CNCS

D1 – **A doutrina existente nas Forças Armadas encontra-se devidamente atualizada?** (…) uma peça doutrinária que é fundamental ainda a ser desenvolvida, que é a ENCD. (…) Até fins de setembro, foram desenvolvidos os princípios orientadores (…). estará em alinhamento com a ENSC 2019-2023.

D2 – **Neste momento existe diversa legislação nos três ramos e no EMGFA referente à CD. Em qual dos modelos apresentados, haveria poupança de recursos humanos afetos à atualização da legislação?** (…) o modelo de haver um só CSIRT com elementos, ou com equipas de resposta nos ramos, eventualmente sob direção técnica do CSIRT central, era claramente o melhor modelo. Deixando aos ramos aquilo que é específico dos ramos.

D3 – **Qual dos modelos considera que irá garantir uma maior uniformização da legislação operacional e tática que está preconizado desenvolver?** (…) o modelo da centralização porque poderia haver (…) uma camada da legislação comum a todos e depois uma regulamentação, ou normas técnicas específicas para casos específicos (…) a taxonomia seria comum e isso facilitaria muito a IO.

D4 – **Qual dos modelos facilitará a normalização da condução de operações no ciberespaço?** (…) seria naturalmente o modelo que facilitaria mais a criação por exemplo do que nós chamamos as SOP, que em função de determinados cenários pré-definidos garantiria uma resposta adequada e mais eficaz e também mais eficiente de ser executada (…) com o modelo centralizado haveria menos entidades envolvidas na resposta portanto a resposta seria, (…) mais eficiente, menos pessoas para atingir o mesmo objetivo. (…) temos de ter juristas especialistas em CS e em CD e em regras de empenhamento. E é muito mais fácil (…) tê-los numa equipa centralizada do que ter vários espalhados pelos ramos.

D5 – **Quais as vantagens e desvantagens, no âmbito doutrinário, não abordadas anteriormente, que considera pertinentes de referir em cada um dos modelos explanados? Como as desvantagens podem ser superadas?** (…) Sendo a raiz da doutrina comum, com apenas diferenciações ao nível específico, há uma coerência doutrinária que ajuda também a criar doutrina nas próprias FFAA. (…) se não houver segurança no ciberespaço não há desenvolvimento económico. E as FFAA servem para garantir segurança. (…) a desvantagem maior é ir contra a cultura vigente. (…) era mais fácil se calhar, inicialmente, desenvolver uma capacidade própria sem ter de alinhar com quem quer que seja. Mas no ciberespaço, não se pode estar sozinho. Nós aqui, (…) no CNCS (…) estamos permanentemente em rede com os CSIRT nacionais. (…) se a doutrina for desmembrada, cada um tiver a sua, (…) quando for necessário as pessoas agirem e interagirem umas com as outras, elas não sabem interagir. (…) com a atual situação de RH, com a falta deles, cada organização ter o seu CSIRT, com todas as capacidades, eu acho que não é bom caminho. É muito caro e é extremamente ineficaz.

O1 – Qual dos modelos considera que melhor contribui para a integração da componente cibernética nas operações conjuntas correntes? (…) claramente um modelo conjunto, mas veja, os ramos, por sua vez também precisam, nos respetivos comandos operacionais (…) de uma célula de resposta a incidentes de CS.

O2 – Quais os maiores desafios organizacionais com a junção dos CIRC num CIRC comum? Como poderão ser superados? (…) Os desafios (…) apesar de serem todos das FFAA, terem hábitos, posturas um bocadinho diferentes. (…) o que eu defendo num futuro é que haja em Portugal, um espaço físico, que tenha o CCD, o CNCS, a unidade nacional de combate ao cibercrime tecnológico (UC3T) e a componente de Intel, que pese embora dependam hierarquicamente das entidades de que hoje dependem, trabalhem no mesmo espaço, incluindo o facto de terem uma mesma sala de operações.

O3 – **(Semelhante D5)** (…) se for garantida no modelo centralizado uma pequena célula *deployable* [RRT] no ramo, com indivíduos do ramo, essa célula pode continuar sob dependência técnica do CCD, (…) recebe normas técnicas, orientações técnicas deles, mas estar sob comando operacional do ramo (…) Mas isto também implicaria que quem chefia o CCD, se calhar tinha de ser um *flag officer*.

T1 – **Neste momento quem determina as formações e treino necessários para cada cargo do CIRC?** (…) Não sei se requisitos dos ramos são enquadrados pelos requisitos do CEMGFA, não sei.

T2 – **Neste momento, os operadores, com funções idênticas nos diversos CIRC, possuem formação semelhante? Os requisitos em cada CIRC são semelhantes? Como contribuir para a sua uniformização?** (…) Nós tendemos a ter formação semelhante. Agora ao nível da defesa não sei.

T3 – **Qual dos modelos considera que melhor contribui para o esforço contínuo de sensibilização para a segurança no ciberespaço?** (…) parece-me que o descentralizado é o mais eficaz.

T4 – (Semelhante D5) (…) o modelo centralizado, tem mais gente, por isso em princípio teria mais capacidade para fazer sensibilização e treino. Só que ao mesmo tempo está mais afastado da realidade. (…) Há requisitos gerais que tem de ser o CSIRT geral a dizer, mas depois as especificidades têm de ser sempre adequadas a cada ramo.

M1 – **Qual dos modelos considera que melhor contribui para a consolidação dos parques informáticos e redes da Defesa Nacional?** (…) temos de garantir que o equipamento está na lista de material aprovado ou pela NATO ou pela UE para tratar informação classificada NATO ou UE. (…) Devia haver uma lista de *approved material*, (…) dentro do qual a aquisição era feita. (…) Tem de haver uma governação (…) onde todos, os responsáveis dos três ramos, do EMGFA e do MDN se sentam.
M2 – **Qual dos modelos considera que melhor contribui para a harmonização de soluções tecnológicas das redes da Defesa Nacional?** (…) é o modelo onde a governação seja centralizada (…) e a execução seja descentralizada. Com normas de *procurement*, portanto, de aquisição semelhantes.
M3 – Qual dos modelos considera que melhor contribui para a uniformização e aquisição de plataformas de treino? É o centralizado (…) É muito mais fácil comprar um *cyber range* e colocá-lo num só local com uma equipa que gere aquilo e depois é usado pelos três ramos, pelo EMGFA (…) do que cada um querer ter o seu *cyber range*.
M4 – Qual dos modelos considera que melhor contribui para a elaboração de um plano de aquisição e sustentação que garanta a uniformização e atualização das plataformas da capacidade de CD, eliminando redundâncias, garantindo vantagens económicas? O central. Aliás, até a capacidade de CD é centralizada, na LPM. Porque é uma capacidade conjunta.
M5 – (Semelhante D5) tem de haver ali dispositivos, que só quem conhece muito bem os navios, a sua arquitetura de sistemas de informação (…) Isso tem de ser visto especificamente.
Mas, onde eu acho que deve ser centralizado com unidades orgânicas *deployable* [RRT] junto dos ramos, em permanência ou *case by case basis*, é a componente operacional.

L1 – Considera que as lideranças dos ramos estão recetivas para uma solução conjunta, deixando de ter sob o seu controlo essa valência? (…) Se essa estrutura conjunta for recetiva a requisitos dos ramos que depois são projetáveis nos ramos, (…) provavelmente haverá essa capacidade.
L2 – (Semelhante D5) (…) já expliquei isto no complemento da resposta anterior.

P1 – As existências previstas no Plano de Desenvolvimento da capacidade de CD contemplam a capacidade CERTDEF? Em caso negativo, quais as existências que prevê como necessárias para garantir a capacidade CERTDEF, bem como as outras necessidades previstas nas incumbências dos CIRC, até 2021? (…) eles têm investido bastante, (…) na componente pessoal da capacidade de CD.
P2 – Considera que as necessidades de RH do CCD plasmadas no "Plano" garantem o CERTDEF? Em que é que essas necessidades poderão ter impacto nos CIRC dos ramos? (…) eu sei que o senhor Almirante CEMGFA tem a ideia de aumentar de forma muito significativa a quantidade de pessoas que vão estar no CCD. (…) deixo esta pergunta para ser respondida objetivamente por outro entrevistado que não eu.
P3 – Quais as iniciativas considera importantes no propósito de garantir uma adequada gestão de carreiras, nomeadamente no que concerne à sua progressão, quer esta seja vertical ou horizontal? (…) a permanência das pessoas nesta área tem de ser longa. (…) formar pessoas com estas competências é muito caro. Um curso da SANS que é uma das entidades melhores (…) na Europa, uma semana custa cerca de 10000€. (…) por terem outras competências, não devem, teoricamente, ser prejudicados na sua progressão na carreira. (…) misto de vertical com horizontal, ou seja, eles podem ir progressivamente tendo outras funções. (…) eles podiam ter funções na entidade do ramo, e depois iam para a CD e depois podiam ir para a escola, para a NCIA ali em Oeiras e depois logo decidiam se queriam continuar nesta área ou dedicar-se a outra, podiam vir para o CNCS também no processo, portanto, tinham várias opções.
P4 – Num mercado tão concorrido e com RH tão especializados, qual prevê ser a melhor forma de contratar RH civis para a CD? E a sua manutenção na instituição? (…) eles têm de ser mais bem pagos. (…) aliciados logo à saída dos politécnicos e das universidades e dos IEFP. Só em Portugal, dizem (…) que existe a falta de 15000 especialistas em CS. (…) obrigatoriedade de eles estarem na organização, função dos cursos que têm, para darem retorno, e há também o aliciamento, não só monetário, mas também com carreiras interessantes.
P5 – (Semelhante D5) O modelo centralizado, com um *procurement* de pessoas centralizado, era capaz de ser melhor. Porque se não for assim, andam-se uns a canibalizar uns aos outros. (…) muito mais vantagens em termos de eficácia e até de eficiência, com o modelo centralizado de recrutamento de pessoal. Civil em particular. (…) corria o risco de se estar a mandar formar várias pessoas com as mesmas competências, eventualmente, o mesmo curso, mas depois não tinha a economia de escala.

IE1 – Sendo necessário, com o aumento previsto de capacidades e de RH do CCD, identificar e alocar IE para acomodar o CCDFA, considera como uma mais-valia a possibilidade de utilização das atuais IE onde estão sediados os CIRC dos ramos, no caso de se avançar para uma solução conjunta? Talvez fosse interessante, no desenhar do futuro *Campus* da Defesa, pensar-se logo numa estrutura que acomode isto.

IE2 – (Semelhante D5) Se for separado, nesta edificação de IE sai tudo muito mais caro. E nunca se faz tão bem. (…) sendo que cada ramo (…) deverá ter uma capacidade orgânica mínima que possa projetar com as suas forças operacionais (…)
IO1 – Qual dos modelos apresentados considera como uma mais-valia na otimização do processo de partilha de informação, dinamizando o mesmo e diminuindo as vulnerabilidades mútuas? (…) se a IO for um requisito à cabeça, qualquer um dos modelos dá. Agora se não for, obviamente que o centralizado é melhor. **IO2 – Considera viável ao nível de IO entre redes e sua monitorização a junção dos CIRC dos ramos num CIRC conjunto? Em caso negativo, como superar esse desafio?** (…) tecnologicamente podem-se monitorizar redes num só centro de operações da rede. Isso sem dúvida nenhuma. Agora eu pergunto é se isso é resiliente. (…) se uma pessoa atacasse aquele único ponto podia comprometer a própria segurança da rede. (…) centros de monitorização cujo *output* depois podia ser visionado ao nível de um CIRC conjunto. **IO3 – (Semelhante D5)** (…) nada de relevante se faz sozinho. (…) um individuo tem de ser interoperável com os seus pares. Tem de se falar todos a mesma língua, (…) os sistemas tecnológicos têm de ser interoperáveis, a taxonomia. (…) Tem de haver procedimentos comuns. Isso é fundamental. (…) A desvantagem é tão grande que equivale a nada disto funcionar.

Tabela 4 – Resumo entrevista CMG Fialho de Jesus/CFR Câmara de Assunção – CCD

D1 – Não. No que respeita ao EMGFA, a doutrina (…) remonta ao ano de 2008. **D2** – Independentemente do modelo adotado, (…) a doutrina operacional para a CD será única e será desenvolvida por elementos do CCD em conjunto com elementos dos Ramos, por forma a garantir o alinhamento de todos. **D3** – Ver resposta anterior. **D4** – (…) qualquer que seja o modelo adotado, a doutrina a desenvolver para a condução de operações no ciberespaço será toda alinhada entre os ramos e o CCD. **D5** – NIL
O1 – (…) o modelo de CIRC distribuídos permitirá uma ter uma maior proximidade do CIRC com a equipa de administração dos sistemas de informação por forma a mitigar os incidentes. **O2** – (…) a aplicação da competência de autoridade técnica que estaria a ser exercida pelo EMGFA (...). **O3** – NIL
T1 – O plano de formação encontra-se a ser desenvolvido (…) A execução deste plano de formação estará a cargo do CCD. No que respeita ao treino coletivo, o CCD é responsável **T2** – Uma das ações a desenvolver no âmbito do "Plano" é o desenho de um QO similar (…) O plano de formação (…) será baseado no desenvolvimento de conhecimento, perícias e habilidades **T3** – Não creio que existam diferenças (…). **T4** – NIL
M1 – Nenhum. Os parques informáticos e redes da Defesa Nacional não são da responsabilidade da CD **M2** – (…) existe a intenção de uniformizar estas soluções por forma a rentabilizar o investimento na formação (…) e ganhar economia de escala (…) o CCD e os CIRC dos ramos têm trabalhado sempre em conjunto para definição das melhores arquiteturas a adotar. **M3** – Independentemente do modelo, a plataforma de treino será uma só para servir a capacidade de CD **M4** – (…) independentemente do modelo adotado, as plataformas da capacidade de CD são pensadas e definidas em conjunto, e são adquiridas e sustentadas pelo CCD **M5** – NIL
L1 – É natural que uma rentabilização de recursos do modelo de CIRC conjuntos possa parecer como uma boa ideia, no entanto têm de ser ponderados os prós-e-contras desta situação, nomeadamente a questão da proximidade com as equipas de administração de sistemas e a flexibilidade na utilização dos recursos. **L2** – NIL
P1 –Esta organização possibilitará a operação 24/7 para a monitorização e investigação preliminar de incidentes de segurança da informação. Não foi desenhado um QO fixo. Ainda não estão perfeitamente definidas as necessidades de pessoal por cada turno (…) atingir a *Initial Operational Capability* em 2021 esta capacidade já seja uma realidade. **P2** – (…) é difícil afirmar que os recursos idealizados garantem o CERTDEF, mas estou convencido de que sim. O reforço da capacidade de CD, em termos de RH, terá sempre impacto nos Ramos, estes recursos já com as competências necessárias são praticamente inexistentes. **P3** – (…) garantidos um conjunto de cargos funcionais nos diferentes patamares que garantam uma progressão de carreira até ao topo, no que aos oficiais diz respeito. A possibilidade de uma progressão horizontal (…) podendo prolongar a sua permanência no seio da capacidade.

P4 – A contratação de RH civis (…) é uma das formas de mitigarmos a falta de RH militares, (…) também é (…) uma das formas de "perpetuar" o conhecimento na organização militar que tem uma rotatividade elevada. (…) uma das formas de contratar pessoal civil é a mobilidade interna na AP (…) patrocínio da formação superior de estudantes (…) garantindo que após a sua formação (…) permanecem nas FFAA durante um período de tempo (…) **P5** – NIL
IE1 – Não. As atuais IE onde estão sediados os CIRC dos Ramos não têm as condições para o quantitativo de militares planeado para as necessidades do CCD. **IE2** – NIL
IO1 – (…) modelo de CIRC conjunto otimiza o processo de partilha de informação pois concentra numa única entidade a produção e publicação da mesma (…) Atualmente, (…) este processo obriga a uma maior coordenação entre as diversas entidades tanto no sentido ascendente como descendente. **IO2** – Viável será sempre, no entanto esta solução trará sempre inconvenientes. (…) proximidade das equipas de resposta a incidentes das equipas de administração de sistemas é uma mais-valia para a celeridade e eficácia da resposta, o distanciamento físico e organizacional traria muitos obstáculos à sua atuação. (…) maximizar a eficácia de um CIRC conjunto (…) restruturação profunda da área das TIC (…). **IO3** – NIL

Tabela 5 – Resumo entrevista TCOR José Teixeira – CCDCOE

D1 – Que eu saiba não existe doutrina ciber aprovada e publicada. **D2** – (…) Com um domínio único, poderá pensar-se em centralizar recursos/capacidades e obter-se uma poupança efetiva. **D3** – Um modelo centralizado. Domínio comum. Regras comuns, procedimentos comuns. **D4** – (…) O modelo centralizado apresentará vantagens (…) na condução das DCO exatamente por terem de ter procedimento comuns, uma vez que o domínio é único independentemente do número de redes e segmentações existentes. **D5** – O modelo centralizado normalmente prevê a constituição de RRTs que são projetáveis para os locais quando o incidente não consegue ser resolvido remotamente.
O1 – A capacidade cibernética tem de ser vista como uma capacidade conjunta, pelo que todas as operações deveriam ser realizadas de forma centralizada. **O2** – (…) mudança de mentalidade em que as telecomunicações permanentes ou fixas passarão a ser vistas como um serviço a ser prestado de forma centralizada (…) implicará uma perda de flexibilidade ou um aumento da dependência dos Ramos. **O3** – O investimento que é necessário em preparar/especializar os recursos humanos que irão alimentar qualquer uma das soluções apresentadas é enorme.
T1 – As formações e treino necessárias para o desempenho de cada cargo deverão estar listadas nas *job description* **T2** – Se a função é igual, a formação de base deve ser igual, podendo caso haja necessidade especializar esses operadores quando haja diferenças no *hardware/software* ou tecnologia utilizadas por cada um dos CIRC **T3** – Não me parece que o tipo de modelo utilizado tenha relação direta com o resultado das ações de sensibilização para a segurança no ciberespaço. **T4** – (…) o modelo praticado em Portugal, já reflete uma certa centralização na gestão e organização do treino. Parte substancial da formação dos CIRC dos Ramos está centralizada no CCD (…)
M1 – A existência de um domínio único com regras de utilização comuns e independentes dos Ramos, tornaria as redes da Defesa Nacional mais fortes. **M2** – Ver resposta anterior. **M3** – plataformas de treino (…) adquiridas, deverão ter em conta as necessidades de todos, pelo que se torna indiferente (…) a uniformização/implementação de políticas comuns favoreça e simplifique a escolha das mesmas. **M4** – Se o processo de aquisição for centralizado (…) mais provável de se assegurar uma aquisição mais abrangente e completa (…) facilidade (…) manutenção das plataformas de treino. **M5** – (…) Não há tecnologias/produtos perfeitos, todas têm os seus pontos fortes e fracos, pelo que a utilização de tecnologia diferente poderá/deverá mitigar lacunas e reduzir vulnerabilidades.
L1 – (…) A perda da capacidade de resposta a incidentes é vista como perda de capacidade de gestão, controlo e independência, pelo que não vislumbro recetividade quanto a uma solução unificada. **L2** – (…) O fluir da informação necessária para que as decisões sejam tomadas da forma mais informada possível (…) irá determinar a forma como se irá organizar/articular seja qual for o modelo utilizado.

P1 – (…) dependência na estrutura do EMGFA (condição muito importante para assegurar a exequibilidade do PRTCERTDEF). **P2** – (…) a função de PRTCERTDEF se encontra perfeitamente identificada na proposta de estrutura organizacional, pelo que as necessidades em termos de RH devem ter sido acauteladas. **P3** – Garantir que algumas das funções a desempenhar no CCD têm equivalência de funções às necessárias para progressão vertical e prever e assegurar a formação necessária para que se consiga ir progredindo vertical e horizontalmente. **P4** – A contratação de RH civis para a CD será extremamente complicada (…) aplicabilidade limitada (…) estabelecimento de contratos de termo definido associados à formação proporcionada e com indemnizações previstas em caso de incumprimento para ambas as partes (…) progressão na carreira associada a capacidades e mérito com respetiva melhoria em termos monetários. **P5** – NIL
IE1 – (…) solução ideal seja a de ter o CCD todo nas mesmas instalações. O estabelecimento de contactos diários entre os vários elementos é fundamental num domínio em que o mais difícil de garantir são relações de confiança. **IE2** – Algo que muitas vezes é descurado são os aspetos de segurança (informação, pessoal e a física).
IO1 – a resposta a incidentes se enquadra como parte das operações defensivas, pelo que a sua responsabilidade deverá ser da entidade autorizada a conduzir operações no ciberespaço. **IO2** – Espero sinceramente que seja essa a solução a ser adotada num futuro próximo. Qualquer solução diferente vai acarretar riscos desnecessários. **IO3** – assegurar a IO com entidades exteriores, tanto nacionais como internacionais (IO tecnológica, mas acima de tudo de taxonomia e processos).

Tabela 6 – Resumo entrevista Coronel Quaresma Rosa – DCSI Exército

D1 – (...) a nível das FFAA eu não considero que exista uma doutrina relativamente ao emprego operacional da CD (…) na inexistência de doutrina nacional, vamo-nos socorrer da doutrina de referência. Doutrina NATO (…) doutrina americana que está um bocado mais desenvolvida e em constante atualização. **D2** – (...) a CD enquanto vertente de segurança, de ações de defesa está enquadrada, em termos nacionais, pela Lei do Cibercrime (…) a Lei dos Conflitos está perfeitamente enquadrável quando há uma situação de crise ou uma situação de guerra declarada, (...) tudo o que são ações de proteção e defesa das redes, têm de ser conduzidas pelas entidades que melhor conhecem as redes e a especificidade das redes. (...) qualquer uma das soluções, em termos de RH empenhados na elaboração doutrinária, a diferença seria muito pouca. **D3** – (...) a doutrina de topo, ela terá de existir (…) As TTP também (...) em termos de redes táticas (...) há coisas que são diferentes. (...) se ela estiver centrada ou se estiver descentralizada em termos de estrutura doutrinária eu penso que ela vai ser muito idêntica em termos de RH. **D4** – Modelo centralizado em termos de ofensivas (...) As de defesa, (...) isso é uma coisa de quem conhece a rede (...) e isso é descentralizado. **D5** – (...) existe a necessidade de haver uma doutrina de topo, conjunta e depois o desenvolvimento (...) das TTP (...) ao nível de componente (...)
O1 – (...) se (…) é responsabilidade do Exército em aprontar a força, a capacidade de CD deverá ser o Exército a fornecer. Se é uma força de natureza puramente conjunta (…) a capacidade de CD (…) terá de ser uma capacidade conjunta (...) **O2** – (...) se (...) as orientações nacionais e a análise do ambiente for para tornar a CD (..) como é a Holanda (…) em que têm tudo centralizado (...) vai ser como é que esse órgão centralizado vai adquiri as competências e os conhecimentos necessários para fazer face às especificidades de cada um dos ramos. **O3** – (...) cada ramo tem as suas especificidades que deverá ter uma estrutura orgânica própria. Podemos questionar a dimensão dessa estrutura, e as tarefas atribuídas a essa estrutura, mas ela terá de existir (…) ao nível do EMGFA deverá de haver uma capacidade mais ou menos robusta para conduzir todas as outras ações que não caem nas competências de cada uma das entidades dos ramos.
T1 – não existe um *job description* (...) da análise das necessidades de adquirir determinadas competências, nós identificamos determinadas formações que vão ser dadas. E depois introduzimo-las em planeamento, umas vezes são financiadas, outras vezes não (…) Existe uma outra vertente da formação que é disponibilizada através do CCD (…) apesar de haver o anunciar de que é uma prioridade, depois não se vê essa mesma prioridade refletida nos outros planos (afetação de RH e financeiros). **T2** – Eu julgo que as formações são mais ou menos semelhantes (...) Claro que depois há determinadas especificidades de cada ramo e determinadas soluções implementadas por cada ramo que obrigam a ter formação díspar em determinadas tecnologias (...) **T3** – O descentralizado (...) na condução de ações de sensibilização presenciais (...) ações de sensibilização partindo de plataformas (...) é independente estar centralizada ou estar distribuída (…)

T4 – (...) oportunidades de treino conjunto numa estrutura centralizada se calhar seriam maiores (...) descentralizada existiam mais situações de treino específicas (…) e menos conjuntas (…)
M1 – (…) não é algo que se consegue centralizando ou descentralizando a capacidade de CD (…) A CD por arrasto poderia ser centralizada se houvesse uma rede única da defesa com um parque informático da responsabilidade da Defesa. (...) Isso será decisão política de partir para uma integração das redes e dos sistemas (...) **M2** – (...) este aspeto das tecnologias e dos equipamentos e das soluções tecnológicas, elas já estão harmonizadas (...) consegue-se isso através da utilização de plataformas que são interoperáveis ou que são as mesmas plataformas utilizadas descentralizadamente (...) apesar das entidades estarem descentralizadas, a estrutura tecnológica está bem centralizada. **M3** – (...) Em termos de economia de escala, eu adquiro uma instância que me permita ter módulos destinados a cada um dos ramos. Ela tem vindo a ser centralizada se bem que depois a execução é descentralizada. **M4** – (...) em termos de aquisição e definição de requisitos e economias de escala uma solução centralizada é sempre mais vantajosa. **M5** – (...) tem de existir essa capacidade projetável, que poderá, na essência ser diferente de ramo para ramo face à especificidade de cada um dos ramos (...) Ao nível da rede administrativa, (…) poderemos evoluir e poderá se pensar em centralizar, mas vai ter de se ter sempre uma descentralização das redes táticas (...)
L1 – Não. Do que eu me tenho vindo a aperceber, existe uma grande preocupação que os ramos percam essas valências e que passem a ser uma valência conjunta. **L2** – (...) Isto é tudo uma questão de interesses e de orientações politico-estratégicas que estão na cabeça de cada um dos chefes (...) o que é certo é que cada um tem vindo a lutar para que se mantenha no seio dos ramos esta capacidade, mais que não seja residual (…)
P1 – Não. Porque não temos possibilidade de ter pessoal 24x7 (...) o QO tal como está me possibilitaria implementar, em termos de 24x7 a existência de um *watchkeeper* em permanência, mas depois a capacidade de resposta *on-call*. (...) Pressupostos: colocarem-me aqui o meu efetivo total de 5/6/3 e garantirem-me que o pessoal só desempenha a escala técnica. **P2** – Sim (...) Os 90 elementos quando foram identificados foram pensados tendo em mente o nível de ambição de ter 24x7. (...) o impacto no Exército (...) ao nível das transmissões é grande (...) **P3** – Enquanto nós não tivermos (…) uma remuneração que seja atrativa, vamos continuar a ter deficiência no recrutamento e na retenção (…) cumprir aquilo que prometemos (...) ponderar o percurso de carreira (...) ponderar o desenvolvimento horizontal (...) (...) arranjar mecanismos em que a progressão vertical até determinado patamar que seja possível dentro da estrutura orgânica (...) Criação de um quadro, de uma especialidade (...) **P4** – Prende-se com (…) a competitividade face ao vencimento. (…) vantagem (…) exercer de uma forma legal (…) atividades ofensivas. (utilização de hackers condenados - não por estas palavras) **P5** – (…) existe a vantagem de ter pessoal civil. (…) Porque (…) é daqueles que dá mais continuidade (…) Porque não está sujeito a determinadas regras para promoção, ou determinadas exigências estatutárias. A dificuldade de recrutamento (…) modelo centralizado as responsabilidades estariam mais centralizadas. definição dos processos de recrutamento e de alvos de recrutamento (…) teria de ser definido centralmente (…) a um patamar superior, MDN, porque são eles que têm a possibilidade de exercer pressão ou alteração de determinados regulamentos.
IE1 – Sob o ponto de vista técnico e de conetividade é indiferente onde é que os CIRC estariam (...) uma solução centralizada obrigaria a uma IE extremamente avultada (...) **IE2** – Tal como está (…) o orçamento, ou o investimento, para melhorar alguns dos requisitos de segurança se calhar são mais baixos (…) Se vamos partir para uma situação de construção de raiz não é aceitável que haja determinados requisitos que não sejam cumpridos e esses requisitos têm custos extremamente elevados.
IO1 – (…) Eu não vejo que o módulo descentralizado ou o módulo centralizado traria vantagens ou inconvenientes em termos de partilha de informação ou em termos de fluxo de informação, mas sim em termos de cultura organizacional e de procedimentos (...) cooperação e colaboração e a partilha é essencial e mandatória. E isso está associado aos processos e às relações de confiança. **IO2** – (...) mais do que uma junção dos CIRC é, nós partirmos para uma estrutura de rede da Defesa e não de redes segmentadas com um interligação (...) há outros valores que se levantam, há outros níveis de ambição que se levantam, há outros aspetos de continuidade operacional, estratégico e político que se levantam, portanto, os *drivers* não são os CIRC (...) **IO3** – (...) Neste modelo descentralizado existe uma grande preocupação em garantir que os sistemas que são implementados que são interoperáveis e que falam entre eles. (...)

Tabela 7 – Resumo entrevista CFR Caldeira de Carvalho – EMA

D1 – A doutrina encontra-se completamente desatualizada. (…) e é uma doutrina muito volátil, (…) tem de haver uma doutrina enquadrante (…) e depois tem de ser feita com muitos normativos operacionais que permitam ser facilmente adaptados às novas ameaças (…) é preciso atualizar toda a doutrina, portanto, o topo até a tática, a operacional e a tática. **D2** – (…) o facto do EMGFA, que é a entidade conjunta que devia fazer supervisão ter muita falta de RH e não ter efetuado a legislação enquadrante que devia ter feito. (…) a legislação superior vai obrigar a dar tarefas específicas enquadrante dos ramos, (…) se não houver necessidade de haver CIRC's complexos, se só tivermos equipas de reação rápida nos ramos, a doutrina que eles vão utilizar é a doutrina do CCD **D3** – os ramos só fazem proteção das suas redes (…) a parte ofensiva está reservada neste momento ao CCD porque os ramos não têm capacidade para fazer parte ofensiva neste momento. **D4** – Os dois modelos podem fazer uma normalização desde que seja imposto superiormente. Mas sem dúvida nenhuma, se tivermos um CIRC centralizado, que vai ser muito mais fácil impor essa normalização. **D5** – (…) Se houver um modelo centralizado, é tudo muito mais uniforme, vão ter de obedecer a padrões já feitos pelo CCD, mas terá de sempre haver normas específicas para cada ramo (…) no caso dos núcleos CIRC descentralizados, terá de ser o núcleo CIRC responsável por essa normativa, mas se for centralizado, vai ter de ser sempre pessoal do ramo a fazer essa parte de especificação. (…) A vantagem é que se for o núcleo CIRC do ramo, vai ter um Almirante que vai influenciar diretamente normativo e poderá requerer mais recursos internos para esse normativo, e se for no CCD isso varia conforme o ramo (…) ele vai ter que deixar ao critério das equipas e não vai pôr imposição de recursos, aliás, ele quer é minimizar os recursos de cada solução
O1 – Nas operações correntes, é sem dúvida a parte centralizada (…) Nas operações específicas de cada ramo, é a parte descentralizada (…) tem de haver uma descentralização do planeamento operacional de missões específicas dos ramos na parte cibernética pelo menos. **O2** – (…) Os desafios organizacionais é somente o ego do ramo porque perde uma série de autonomias. Não há desafios organizacionais, aliás, é mais fácil, requer menos RH e requer menos recursos materiais. (…) vamos ter um CIRC central a dar regras e instruções gestão das redes específicas do ramo e os ramos não gostam disso. **O3** – (…) A única desvantagem que há (…) é a falta de RH. (…) Se nós tivermos um modelo centralizado, grande e robusto (…) temos equipas só residuais nos ramos, (…) temos só uma dificuldade que é a rotação dos meios humanos.
T1 – (…) a formação, tentativamente vai ser comum, (…) porque a formação é cara e os números compensam. **T2** – (…) não são semelhantes nem há formação semelhante. (…) o CCD definir centralmente, para desempenhar que cargo, qual é a formação que tem de ter, e é o que está a ser feito **T3** – (…) não há diferença entre os modelos porque isto é muito mais uma política institucional (…) Quando estiver centralizado, vai haver verificações e um esforço para haver uma sensibilização de todos os utilizadores do domínio da defesa, incluindo a Marinha, o Exército e a FAP. **T4** – (…) é aqui fundamental é definir uma matriz de formação por função, por nível de função. (…) está definido a nível da NISC e da UE, estão definidos para funções, quais são os KSA que cada função requer, consoante o nível que requer. (…) Isso acho que é o principal passo a dar agora que estamos muito no principio.
M1 – (…) Sem dúvida a parte centralizada. (…) ter o CIRC que é responsável por isso, da segurança das redes da Marinha estar debaixo do almirante que é responsável pela gestão das redes da Marinha, estamos a condicionar. (…) a segurança nunca devia estar sob (…) chapéu do mesmo chefe que (…) faz a gestão de redes. (…) Para garantir a segurança das redes é melhor ser uma coisa centralizada. **M2** – Já respondido na pergunta anterior. **M3** – É o centralizado. Tudo isso aí é centralizado. (…) A aquisição de plataformas de treino, na CD são coisas caras. O *cyber range* são coisas muito caras que têm de ser altamente rentabilizadas. (…) não é aceitável que cada ramo compre a sua. **M4** – A centralização é sem dúvida isto, mas neste momento, na parte das plataformas de capacidade de CD, já há uma centralização. (…) o CCD está a fazer aquisição centralizada. (…) Mas os ramos têm autonomia para propor soluções delas, o que para mim é um erro. **M5** – (…) centralização de aquisição. (…) aquisição e centralização de todo o material de redes das FFAA deve ser centralizado e adquirido centralmente.
L1 – (…) A grande oposição de uma solução deste tipo é sem dúvida os ramos e os chefes dos ramos que não querem perder valências nem a capacidade de gestão das suas próprias redes. Portanto não estão. Tem de ser um papel de mentalização superior ou imposição.

L2 – (…) Eles têm de ter essa consciência (…) Tem de haver confiança e tem de haver desprendimento. Têm de perder algumas valências. (…) E mais cedo ou mais tarde vai acontecer. Ou vão fazer voluntariamente ou vai ser imposto.
P1 – (…) o "Plano" já prevê o CERTDEF. (…) Se os ramos derem o pessoal com as valências necessárias e for possível dar as valências necessárias ao pessoal, em 2021 (…) já estão 24 sobre 7 e já podem substituir os CIRC. **P2** – (…) como não há pessoal, neste momento para o CERTDEF ter o pessoal que necessita vai ter de esvaziar os CIRC dos ramos. (…) isto é uma valência de extrema importância, (…) que os chefes têm de ter noção que afeta a sua capacidade operacional e afeta o cumprimento da missão dos ramos e da defesa. **P3** – (…) O pessoal de EM (…) deve gostar pelo menos do assunto e ter uma vocação para isso, mas não tem de ter um conhecimento técnico aprofundado, aliás, misturar as duas coisas é mau. (…) Este pessoal técnico é pessoal muito especializado e muitas vezes a grande motivação deles é o desafio e o conhecimento e o conseguirem fazer mais coisas. (…) principalmente este pessoal, não vai ter capacidade de cumprir que são previstos no EMFAR para a carreira normal do militar. (…) temos de definir uma carreira horizontal e temos de definir condições especiais de promoção para esses elementos. (…) se calhar vamos ter de garantir um suplemento especial a esses elementos. (…) não conseguimos competir com as empresas lá fora. (…) têm de ter uma carreira horizontal e ficar no mesmo local, se calhar, 15 anos. **P4** – (…) É muito difícil a não ser que tu lhes dês uma série de contrapartidas, (…) suplementos especiais, e lhes garantas formação contínua e desafios contínuos. (…) dando uma carreira que seja aliciante e desafiante (…) para esse pessoal. (…) um fator primordial (…) é o fator remuneratório **P5** – (…) uma solução economicista, uma solução centralizada, de certeza que requer menos recursos. Se a gente tivesse RH infinitos, lógico, que ter um comando de CD em cada ramo e teres um central, era o ideal. Mas isso tinhas de ter RH infinitos, recursos financeiros infinitos para treinarmos o pessoal.
IE1 – (…) Tem de estar tudo junto. Não funciona. A CD funciona, e a CS funciona muito em fórum de equipas. (…) Isto também se baseia muito na experiência pessoal (…) e isto só funciona bem se estivermos todos juntos e falarmos e trocarmos ideias e ouvirmos os outros. (…) Tem de se acomodar nas estruturas, agora vai-se dar mais um piso do, lá do ministério e tem de ficar tudo junto. **IE2** – temos de estar em equipa e temos de partilhar as ideias. a partilha de ideias é fundamental nesta área.
IO1 – (…) uma parte centralizada é sempre uma mais-valia, para partilha de informação, estamos todos no mesmo sítio, a ver todos os mesmos quadros e estamos a ver todos a mesma coisa. (…) descentralização, (…) requer mais trabalho e a informação é filtrada antes de ser divulgada. Sempre. **IO2** – (…) CCD já tem capacidade de monitorizar todas as redes. Há lá uns *blind spots*, mas já estavam (…) a ser resolvidos. (…) Um passo que tem de se dar para a segurança das redes, (…) é a unificação das redes que é um passo que também tem grandes desafios na liderança, não é tecnicamente. Tecnicamente é fazível e é viável e não é difícil de fazer. Mas em termos de liderança é complicado. **IO3** – (…) na parte centralizada consegue-se ter muito mais contacto, (…) não só (…) da defesa, mas também com a parte da segurança em si com o CNCS. (…) Se tivermos uma coisa mais centralizada. E não haveria tantas barreiras invisíveis como existe neste momento.

Tabela 8 – Resumo entrevista MAJ André Castro – CIRC FAP

D1 – (...) como é uma temática ainda muito recente é natural que a parte documental não acompanhe a evolução tecnológica. **D2** – (...) numa abordagem centralizada pudesse haver poupança de trabalho a nível da produção de documentação. Obviamente que cada ramo tem as suas particularidades (…) mas iria envolver (…) provavelmente os mesmos RH. **D3** – (...) acredito que uma solução centralizada fosse mais fácil. **D4** – numa solução centralizada é sempre mais fácil de normalizar **D5** – (...) se tivermos um órgão apenas é muito mais fácil produzir legislação enquadrante (…) as particularidades dos ramos levam a que esta uniformização com uma centralização, nem sempre seja fácil. (…) conhecimento mais atualizado e mais ativo das particularidades dos ramos estão nos ramos (…) a nossa proximidade (…) é maior
O1 – (...) numa solução centralizada seria mais fácil de implementar, de contribuir para operações (…) conjuntas **O2** – Um CIRC único acho que estava muito melhor dotado de capacidades de reação (…) se for num centro único essa coordenação possa ser difícil e produzir um efeito nefasto na operação **O3** – (...) o problema maior é sempre o RH. (…) Não sei se, com uma abordagem centralizada ou distribuída, se o investimento em formação (…) se vai ser maior ou menor. Ramos (…) conseguimos ir escolhendo as pessoas (…) e sei quais são as suas valências (…) num centro esse processo de recrutamento se calhar era mais difícil.

T1 – a FAP tem o seu plano de formação. (…) por vezes o centro tem ações de formação que nos disponibiliza **T2** – A formação não é comum por duas razões. Os RH são escassos e eu não consigo ter vários indivíduos formados nas mesmas áreas. (…) as formações nestas áreas são muito caras, consomem muito tempo (…) **T3** – Penso que o modelo descentralizado (…) é mais eficaz. A proximidade (…) é maior (…) **T4** – (...) a formação devia ser superior àquela que existe. (…) Acho que a rotação de pessoal e a formação que é dada, acho que é o grande fator que tem de ser pensado.
M1 – O centralizado, sem dúvida. (…) é muito mais fácil tornar as realidades homogéneas. **M2** – (...) O centralizado, pelos motivos que apontei atrás. **M3** – (...) O centralizado também. (…) Até para poupança de recursos. (…) se forem todas adquiridas pela mesma entidade, centralizada, além de se tornar mais homogéneo, eventualmente até podem ser mais baratas do que estar a dividir isto pelos ramos. **M4** – (...) Sem dúvida o centralizado (…) acho que traria poupanças e em termos os mesmos sistemas (…) grande parte dos equipamentos que os ramos têm (…) foram adquiridos pelo EMGFA. Quando não são, quando são sistemas da FAP, porque nós também compramos os nossos, (…) interligável com o Centro. **M5** – (...) nada a referir
L1 – Não lhe consigo responder a essa pergunta. **L2** – (...) nada a referir. Desconheço
P1 – No novo modelo (…) já está previsto. (…) já foi contabilizado mesmo as horas de trabalho *on-call* e sem ser *on-call*, (…) ir ao encontro dessa expectativa. **P2** – A FAP já contribuiu com o que pôde agora para a primeira leva de militares (…) causou já um grande impacto. (…) o pessoal (…) mais próximos da CD obviamente estão nos CIRC. Não podemos tirá-los daqui enquanto se mantiver este conceito não é, porque senão esvaziamos os CIRC (…) Sim, (…) acho que conseguem cumprir isso sem qualquer problema. (garantia CERTDEF). **P3** – incremento grande na formação, com alguma sobreposição. (…) repensar uma progressão horizontal ou vertical diferente, com menos, (…) restrições, para garantirmos que as mesmas pessoas ficam nos mesmo locais mais algum tempo **P4** – os ordenados, que é um dos motores do recrutamento, é muito forte lá fora (…) recrutamento externo nas faculdades (…) recrutar jovens engenheiros. **P5** – (…) Mais investimento em formação.
IE1 – (…) O aproveitamento de IE já existentes, obviamente é sempre uma mais-valia porque traz poupança de recursos financeiros. **IE2** – (…) não tenho nada para me pronunciar sobre isso. Desconheço um pouco como é que vai ser agora as novas instalações do Centro.
IO1 – (…) modelo descentralizado é mais aplicável (…) resposta mais rápida do que propriamente se for algo centralizado. (…) Os sistemas (…) podem ser geridos centralmente, mas a atenção e a ação acho que se for descentralizado conseguimos ser mais rápidos e mais eficientes (…) sabemos (…) qual é o comportamento normal da nossa rede (…) **IO2** – (…) monitorização (…) poderá ser mais vantajosa uma solução centralizada. A nível de reação e tratamento dessa monitorização (…) uma solução descentralizada acho que continua a ser mais vantajosa. **IO3** – (…) solução centralizada, acho que só iria dar frutos positivos (…) quando (…) houvesse essa homogeneidade a nível de legislação, a nível de equipamentos, parque informático, etc., (…) com as tais equipas *deployable* [RRT], poderia ser um caminho fácil de seguir. Como as coisas estão, acho muito difícil, acho extremamente desafiante (…) as coisas mudam e têm de mudar (…) penso que a abordagem que está a ser seguida agora, descentralizada, continuaria a produzir, eventualmente os melhores resultados a nível da segurança dos nossos sistemas.

Tabela 9 – Resumo entrevista CTEN Courela Alexandre – CIRC Marinha

D1 – (…) uma das grandes lacunas que temos atualmente (…) **D2** – (…) Eu procuro (…) ver quais são as *best practice* atualmente implementadas. (…) na NIST (…) a nível da NATO também e digamos que é mais por aí que eu faço a minha gestão. (…) se estivesse centralizado, (…) acho que haveria uniformização em termos de processos, (…) assim como, talvez menos recursos se calhar, na produção da doutrina. **D3** – (…) no modelo centralizado, provavelmente conseguiremos, do que propriamente os vários ramos estarem a produzir a sua doutrina específica. **D4** – (…) sem dúvida que no modelo centralizado, se as pessoas estiverem num espaço e partilharem esse espaço e partilharem informação, (…) De certeza que o rendimento será superior. (…)

D5 – (…) poupança de recursos, (…) há um grande desconhecimento em termos de procedimentos dos outros ramos assim como a escassez de doutrina e também indefinição em termos de procedimentos. (…) havendo doutrina (…) absorvida por todos os ramos, todos teriam de proceder da mesma maneira.
O1 – (…) sem dúvida que o modelo centralizado terá as suas vantagens, tendo em conta que todos os elementos que estão integrados, (…) eu penso que haveria aí uma capacidade muito superior de responder, nomeadamente ao nível da componente operacional e tática se os elementos estiverem centralizados **O2** – (…) seleção dos recursos com valências para o efeito, (…) Este pessoal altamente especializado é muito difícil de agarrar lá fora e com os vencimentos e com o que nós podemos despender, é extremamente difícil. **O3** – (…) arranjar maneira de selecionar pessoal capaz, com valências e competentes na área e eliminarmos o problema da escassez de recursos a nível da CS, penso que, são os pontos fundamentais.
T1 – (…) temos alguns cursos aprovados em termos da Direção de Formação. (…) as formações que o meu pessoal tem tido são definidas a nível do CCD (…) O treino, nós estamos coordenados pelo CCD. **T2** – (…) tenho notado que tem existido, (…) um certo cuidado no CCD de modo a enviar pessoal dos ramos para os vários cursos. **T3** – (…) No modelo descentralizado, (…) existe uma maior proximidade (…) esse contacto. (…) Eu duvido que no modelo centralizado que exista esta capacidade de falar com os ADU [Administrador Domínio Utilizador] das diferentes unidades (…) e passar (…) a nossa mensagem. **T4** – (…) eu acho que devia de haver um maior planeamento em termos de carreira. (…) não há um planeamento e uma orientação de carreira desde o início até ao fim. Isso considero que é uma das grandes desvantagens, no modelo como está atualmente.
M1 – (…) Não somos nós, (…) que definimos ou vamos consolidar os parques informáticos **M2** – (…) no modelo centralizado nós conseguimos poupar em termos de recursos, nomeadamente com a aglutinação das plataformas **M3** – (…) Uma solução única para os três ramos, (…) Todos os nossos SIEM são idênticos, só que temos quatro. Provavelmente bastaria ter um no CCD a ir buscar informação aos ramos. **M4** – (…) Central. (…) o EMGFA adquiriu através do CCD, adquiriu uma plataforma (…) a custos mais baixos de certeza absoluta. **M5** – (…) Acho que não há aqui mais nada que possa acrescentar aqui a esta questão.
L1 – (…) Não te sei responder a esta questão. Isto é uma questão altamente estratégica. **L2** – (…) mesmo que haja uma centralização (…) eu acho que vai ter de haver sempre um núcleo a nível dos ramos.
P1 – (…) Não. Eu acho que muito dificilmente iremos implementar esta capacidade como estamos atualmente face aos recursos. **P2** – (…) penso que sim, se conseguirmos cumprir o que está previsto no Plano, de certeza que iremos ter esta capacidade. (…) tenho consciência que provavelmente haverá elementos aqui do CIRC (…) que terão de ser deslocalizados para o CCD. **P3** – (…) possibilidade de implementar a classe de sargentos e de praças dentro da CD/CS, (…) a especialização de oficiais em CD, (…) implementar os cursos a nível dos cursos de serviço técnico (…) **P4** – (…) o único modo de conseguir aliciar os civis será, sem dúvida, com uma remuneração equiparada com o que se pratica lá fora. Ou subsídios **P5** – (…) É extremamente difícil garantir um quadro de pessoal que garanta a disponibilidade de RH com competências e valências para o efeito, devido à especificidade e o tipo de formação que é necessária para estes elementos. Tem de ser acautelado, (…) a saída deste pessoal após formação (…)
IE1 – (…) Não me parece que seja a melhor solução. **IE2** – (…) terá de ser arranjado um espaço que consiga alojar todos estes elementos. (…) IE em termos de rede, elas já existem, já estão implementadas.
IO1 – (…) o modelo centralizado implica logo um aumento de partilha de informação. (…) eu não conheço os CIRC dos outros ramos. Acho que isto diz tudo, não é? (…) um CIRC centralizado iria sem dúvida garantir que estávamos todos no mesmo espaço e que todos partilhávamos a mesma informação e o mesmo *knowhow*. **IO2** – (…) É claro que é viável. (…) a rede da defesa é acedida nos ramos. O CCD consegue aceder aos equipamentos que estão nos ramos, por isso não é por aí. Isto já existe. **IO3** – (…) teremos de garantir, (…) políticas com procedimentos semelhantes. (…) não existem políticas nem procedimentos similares atualmente. Deveria de haver uma abordagem comum (…) com um conjunto de regras e conceitos que, sem dúvida que deveriam de ser partilhados por todos os núcleos CIRC de modo a aumentar a IO (…) o modelo centralizado, pelo facto de estarmos no mesmo espaço físico (…) sem dúvida que conseguiríamos aumentar a IO.