INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO MAIOR CONJUNTO

2017/2018

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

GESTÃO E SUSTENTAÇÃO DE UM QUADRO DE PESSOAL ESPECIALIZADO NA ÁREA DA CIBERDEFESA E DA CIBERSEGURANÇA

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.

Luis Miguel Gomes Ferreira

Major Cav GNR

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

GESTÃO E SUSTENTAÇÃO DE UM QUADRO DE PESSOAL ESPECIALIZADO NA ÁREA DA CIBERDEFESA E DA CIBERSEGURANÇA

Major Cav GNR Luís Miguel Gomes Ferreira

Trabalho de Investigação Individual do CEMC 2017/18

Pedrouços 2018

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

GESTÃO E SUSTENTAÇÃO DE UM QUADRO DE PESSOAL ESPECIALIZADO NA ÁREA DA CIBERDEFESA E DA CIBERSEGURANÇA

Major Cav GNR Luís Miguel Gomes Ferreira

Trabalho de Investigação Individual do CEMC 2017/18

Orientador: Tenente-coronel ART
Carlos Miguel Siborro Leitão

Pedrouços 2018

Declaração de compromisso Antiplágio

Eu, **Luís Miguel Gomes Ferreira**, declaro por minha honra que o documento intitulado **Gestão e Sustentação de um Quadro de Pessoal Especializado na Área da Ciberdefesa e da Cibersegurança** corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Estado Maior Conjunto 2017/18** 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**,** 08 de maio de 2018

Luís Miguel Gomes Ferreira

Agradecimentos

Os meus agradecimentos são dirigidos a todos aqueles que ao longo da elaboração deste trabalho contribuíram de alguma forma para o seu desenvolvimento coerente com o objetivo a que me propus. A todos os que me ajudaram a superar as dificuldades com que me fui deparando, um sincero agradecimento.

Um agradecimento especial a todos os entrevistados que foram fundamentais para a realização deste estudo. Pela atenção disponibilizada, o tempo que me dispensaram, o interesse que demonstraram no assunto abordado e a simpatia demonstrada, faz com que estes camaradas mais antigos sejam merecedores do meu sincero reconhecimento. Muito obrigado senhores Comandantes, Diretores e Chefes, sem os vossos valiosos contributos, este estudo não seria possível.

Por último, agradecer ao meu orientador, Tenente-coronel Siborro Leitão, pela sua compreensão ao longo de todo o processo, a atenção que deu a todos os assuntos e o apoio que me foi permanentemente disponibilizado.

A todos, bem hajam.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Índice de Quadros

Resumo

O objeto de estudo do trabalho centra-se na concetualização de um modelo de Gestão de Recursos Humanos Ciber, adaptado às Forças Armadas portuguesas, alicerçado nos vetores da seleção, formação e treino e retenção. Da retenção, foram abordados os aspetos relacionados com a gestão, desenvolvimento pessoal, carreira, tempo de permanência e remuneração.

Neste contexto, adotou-se uma estratégia de pesquisa qualitativa que, pela inexistência de um enquadramento concetual inicial, nos levou à descoberta de uma lógica indutiva, assente num desenho de pesquisa de estudo de caso, com base no *Mando Conjunto de Ciberdefensa* das Forças Armadas espanholas.

O estudo permitiu a concetualização de um modelo de Gestão de Recursos Humanos Ciber que assenta no âmbito da seleção, num modelo misto, com recurso a militares e a pessoal civil, na implementação de um plano de formação, na continuação da participação em exercícios e na criação de uma especialização Ciber fundamental nas Forças Armadas.

Dado que a criação de um Quadro Especial Ciber não faz sentido, a retenção ganha importância, passando pela adoção de uma gestão diferenciada que preserve estes recursos em funções na área, possibilitando o desenvolvimento pessoal, a carreira técnica, aumentando o tempo de inamovibilidade e melhorando o índice remuneratório.

Palavras-chave

Ciber, Gestão de Recursos Humanos, Seleção, Formação e Treino e Retenção

Abstract

The object of study of this work is centered on the conceptualization of a Cyber Human Resources Management model, adapted to the reality of the Portuguese Armed Forces, which is based on the vectors of selection, training and retention. From the retention, were addressed aspects related to management, personal development, career, length of stay and remuneration.

In this context, a qualitative research strategy was adopted that, due to the lack of an initial conceptual framework, led us to the discovery in an inductive logic, based on a case study research design, based on the Joint Cyber Defense Command, of the Spanish Armed Forces.

The study allowed the reconfiguration of a cyber Human Resources Management model that rests in the scope of the selection, in a mixed model, using military and civilian personnel, a training plan must be devised and implemented, continued participation in exercises and created a fundamental Cyber specialization in the Armed Forces.

Since the creation of a Special Cyber Frame does not make sense, retention gains importance, through the adoption of a differentiated management that preserves these resources in functions in the area, enabling personal development, enabling the technical career, increasing the time of immobility and improving the compensation index.

Keywords

Cyber, Human Resources Management, Selection, Training, Retention

Lista de abreviaturas, siglas e acrónimos

CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CC	Comando Ciber
CCD	Centro de Ciberdefesa
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CD	Ciberdefesa
CERT	*Computer Emergency Response Team*
CIRC	*Computer Incident Response Capability*
CNA	*Computer Network Attack*
CNCS	Centro Nacional de Cibersegurança
CND	*Computer Network Defense*
CNE	*Computer Network Exploitation*
CNO	*Computer Network Operations*
CO	Comando Operacional
ComDCiber	Comando de Defesa Cibernética
CRP	Constituição da República Portuguesa
CS	Cibersegurança
DCSI	Direção de Comunicações e Sistemas de Informação
DIRCSI	Direção de Comunicações e Sistemas de Informação
DN	Defesa Nacional
EB	Exército Brasileiro
EUA	Estados Unidos da América
EMFAR	Estatuto dos Militares das Forças Armadas
EMGFA	Estado-Maior General das Forças Armadas
ENaDCiber	Escola Nacional de Defesa Cibernética
ENSC	Estratégia Nacional de Segurança do Ciberespaço
ECSI	Escola de Comunicações e Sistemas de Informação
FA	Força Aérea
FFAA	Forças Armadas
GRH	Gestão de Recursos Humanos
IC	Infraestrutura Crítica
IUM	Instituto Universitário Militar
INFOSEC	*Information Security*
IOC	*Initial Operational Capability*

Kdo CIR	*Kommando Cyber-und Informationsraum*
LO	Lei Orgânica
MCCD	*Mando Conjunto de Ciberdefensa*
MDN	Ministro da Defesa Nacional
MNCDE&T	*Multinational Cyber Defense Education and Training Project*
NATO	*North Atlantic Treaty Organization*
OE	Objetivo Específico
OPC	Orientação Política para a Ciberdefesa
OTAN	Organização do Tratado do Atlântico Norte
PECCN	Plano para a Edificação da Capacidade de Ciberdefesa Nacional
QC	Questão Central
QD	Questão Derivada
QE	Quadro Especial
QEC	Quadro Especial Ciber
QO	Quadro Orgânico
RH	Recursos Humanos
SI	Segurança da Informação
SIC	Sistemas de Informação e Comunicações
SOC	*Security Operations Center*
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
UME	*Unidad Militar de Emergencia*
USCYBERCOM	*U.S. Cyber Command*

Introdução

O presente trabalho de investigação individual, realizado no âmbito do Curso de Estado-Maior Conjunto, do Instituto Universitário Militar (IUM), tem por objetivo estudar em contexto académico a necessidade de criação de um Quadro Especial Ciber (QEC) para integrar os militares das Forças Armadas (FFAA) que desempenham funções em Ciberdefesa (CD) e na Segurança da Informação (SI). O tema insere-se na área das ciências militares, relativamente ao desenvolvimento das metodologias e processos de edificação e emprego de capacidades militares, e no âmbito da administração e Gestão de Recursos Humanos (GRH).

Com a reforma da "Defesa 2020[1]" (CM, 2013b), o Governo implementou um conjunto de medidas e racionalizações e definiu o modelo da Defesa Nacional (DN). Esta reforma delineou as capacidades e os quadros de empenhamento das FFAA para a consecução dos objetivos da política de segurança e DN. Uma das orientações específicas emanada por esta reforma, foi a edificação da capacidade de CD, tendo sido criado em 2015, o Centro de Ciberdefesa (CCD), integrado na estrutura do Estado-Maior General das Forças Armadas (EMGFA), nos termos da sua nova Lei Orgânica (LO) (CM, 2014). Foi também prevista a criação de um núcleo *Computer Incident Response Capability* (CIRC) no EMGFA, Marinha, Exército e Força Aérea (FA).

Passados três anos desta reestruturação, estão criadas as condições para rever o funcionamento destas novas estruturas e, no que ao nosso estudo interessa, avaliar se o modelo de GRH adotado é o que melhor se adapta e responde às necessidades exigidas, na ótica da operacionalidade e do cumprimento da missão para a qual foram criadas.

É uma capacidade que assenta no conhecimento e por isso depende de operadores com qualificações e especializações singulares, sendo de considerar que apenas um reduzido número de indivíduos, são possuidores destas capacidades e, portanto, habilitados a este tipo de trabalho. Das tradicionais atividades de GRH, destaca-se o forte impacto negativo que a fraca retenção pode trazer. Por tudo isto, exige-se uma gestão de pessoal capaz de acompanhar os objetivos da organização, que seja eficiente e criteriosa, à altura das exigências da escassez de Recursos Humanos (RH) e que ao mesmo tempo evite perda de produtividade e de qualidade, por via de baixos níveis de satisfação no trabalho.

[1] Trata-se de uma reforma estrutural implementada pelo programa do XIX Governo Constitucional, que visa obter ganhos de eficiência, economias de escala e vetores de inovação com efeitos no curto, médio e longo prazo, centrada na definição e implementação de um modelo sustentável para a defesa nacional e para as FFAA.

De realçar que estes RH, perfeitamente inseridos na instituição militar, possuem expectativas relativas à sua carreira que em determinadas circunstâncias não são coincidentes com as alternativas que a organização oferece. Estamos perante uma situação que carece ser harmonizada, garantindo um enquadramento que sirva as expectativas dos militares e da organização. O enquadramento organizacional poderá ser uma dificuldade por via do enquadramento legislativo e dinâmica dos seus mecanismos de gestão, que podem condicionar o garante destas condições individualmente, materializando-se em perdas para a organização.

Apesar de alguns autores se terem debruçado sobre a temática da GRH e dos quadros especiais, bem como sobre a questão trazida pelas ameaças cibernéticas, dando oportunidade de edificação de novas capacidades e estruturas, concluímos que não haverá nenhuma investigação que relacione estas duas vertentes, no sentido de apurar se um QEC é o que garante uma melhor gestão de GRH. Assim, o nosso desafio será fornecer esse acrescento de conhecimento, conscientes e motivados pela pertinência do mesmo, com aplicação prática, nos recém-criados CCD e núcleos de CIRC.

Considerando a escolha e a delimitação do tema, excluímos a CS no âmbito da GNR, porque o Gabinete de Cibersegurança da GNR, apesar de previsto, ainda não foi criado. A delimitação, procedimento essencial numa investigação, passa por escolher uma determinada parcela de um assunto estabelecendo limites ou restrições para o desenvolvimento da pesquisa pretendida, pelo que se impõe delimitar a nossa investigação em três domínios: tempo, espaço e conteúdo (Santos e Lima, 2016, pp. 43-44).

No que ao espaço temporal diz respeito, optou-se por delimitar esta investigação ao período compreendido entre a criação do CCD, que corresponde à data da entrada em vigor da LO do EMGFA, um de janeiro de 2015, até aos dias de hoje, altura em que termina a fase analítica deste trabalho de investigação.

A investigação incidirá sobre a capacidade de CD do CCD do EMGFA. Uma vez que o CCD é alimentado com recurso aos RH Ciber dos ramos e em caso de resposta a um incidente, são empregues operacionalmente e integram a estrutura do CCD, os ramos serão abordados de forma indireta. A capacidade de CD será avaliada recorrendo à metodologia DOTMLPI-I[2], utilizada pela OTAN, para a edificação de capacidades operacionais, aplicando-a à atual capacidade do CCD.

[2] O acrónimo DOTMLPI-I (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade) refere-se aos componentes básicos da edificação de uma capacidade operacional, desenvolvido pelo Departamento da Defesa dos EUA e adotado pela OTAN.

Quanto ao conteúdo, ela incidirá sobre a GRH afetos às estruturas dedicadas à CD e SI das FFAA, delimitando-se aos aspetos referentes à seleção e recrutamento, formação e treino e retenção. Dos vetores que podem afetar a retenção, aprofundaremos as suas causas, relativamente à gestão própria, ao desenvolvimento pessoal, gestão de carreira, tempo de permanência na função e remuneração.

No seguimento do referido anteriormente, o objeto da investigação do nosso estudo, é apurar de que forma se pode melhorar a capacidade de CD das FFAA, através de uma GRH Ciber mais eficaz. Neste sentido, o objetivo geral do nosso estudo é apurar qual o modelo de GRH que melhor se adequa aos militares especializados em CD e SI das FFAA, de forma a obter ganhos operacionais nesta capacidade.

Para alcançar este objetivo definiram-se os seguintes objetivos específicos (OE):

OE 1: Identificar o impacto que a GRH tem, atualmente, na capacidade operacional de CD das FFAA.

OE 2: Caraterizar o modelo de GRH empregue na capacidade de CD nas FFAA de um país da OTAN.

OE 3: Identificar as medidas que podem ser implementadas na GRH Ciber das FFAA.

Uma das possibilidades para gerir melhor estes RH é, tendo em conta a leitura de trabalhos desenvolvidos nesta área e as entrevistas exploratórias efetuadas a especialistas e responsáveis pela GRH das FFAA, como indicado por Rolo (2009, p. 13), uma gestão orientada por um Quadro Especial (QE), uma vez que ao nível do desenvolvimento da carreira, "*o estabelecimento dos QE se tem mostrado um instrumento importante na satisfação das necessidades para os cargos, ao mesmo tempo que reduz as distorções nas carreiras"*. Considerando este contributo, surge a seguinte Questão Central (QC): Como poderá ser otimizada a GRH Ciber nas estruturas Ciber das FFAA?

Articuladas com a presente QC, desenvolveram-se questões derivadas (QD):

QD 1: Qual o impacto da atual GRH Ciber na capacidade operacional de CD das FFAA?

QD 2: Qual o modelo de GRH empregue no *Mando Conjunto de Ciberdefensa* (MCCD) das FFAA do Reino de Espanha?

QD 3: Quais as medidas que, ao nível da GRH Ciber, podem ser implementadas com vantagens para a capacidade de CD das FFAA?

Através da validação das QD daremos resposta à QC, pelo desenvolvimento de uma estratégia de investigação qualitativa, recorrendo essencialmente ao raciocínio do tipo

indutivo (Santos e Lima, 2016, p. 20). Uma vez que o modelo de GRH Ciber será gerado a partir do estudo do modelo espanhol e dos dados recolhidos dos peritos e não de um enquadramento concetual, criado no início da nossa investigação (Bryman, 2012, pp. 26-27).

Quanto ao desenho de pesquisa a adotar, estabelecemos o estudo de caso do MCCD das FFAA espanholas. A recolha de dados será efetuada recorrendo a fontes documentais e a entrevistas do tipo semiestruturadas, para as quais foi elaborado um guião (Apêndice E), abordando tópicos previamente determinados com interesse para o trabalho (Santos e Lima, 2016, pp. 29-31).

O trabalho aqui introduzido será organizado em quatro capítulos.

No primeiro apresentaremos a base concetual referente à CD e dos profissionais Ciber. No âmbito da GRH, abordaremos os aspetos relativos à seleção e recrutamento, formação e treino e retenção. Apresentaremos ainda o percurso metodológico e o nosso modelo de análise (Apêndice B), que se constitui como guia da nossa investigação.

No segundo capítulo, iremos analisar o impacto que os RH e a sua gestão têm atualmente na capacidade de CD das FFAA, através da aplicação da metodologia DOTMLPI-I ao CCD, aprofundando os vetores relacionados com o pessoal, nomeadamente os processos de seleção, formação e treino e retenção, respondendo à QD1.

No terceiro capítulo, que corresponde ao nosso estudo de caso, o MCCD das FFAA espanholas, iremos analisar, através da metodologia DOTMLPI-I, o modelo de GRH adotado por este país amigo, respondendo à QD2. Adicionalmente e de forma sucinta serão também referenciadas as abordagens dos Estados Unidos da América (EUA), do Brasil e da Alemanha (Apêndice A).

No quarto capítulo, analisaremos o contributo que as medidas, a implementar ao nível da GRH Ciber, garantem na melhoria da capacidade de CD das FFAA, de forma a obter resposta à QD3.

Terminaremos a nossa investigação, procurando avaliar se os objetivos específicos e geral foram atingidos, assegurando as respostas às QD e consequente resposta à QC. Serão propostas medidas, materializadas num modelo de GRH Ciber, para melhoria da capacidade operacional de CD e direções para futuras investigações.

1. Enquadramento concetual e percurso metodológico

Neste capítulo, iniciaremos por enquadrar o nosso estudo no âmbito dos conceitos de ciberespaço, SI, Cibersegurança (CS) e CD. Seguidamente, faremos uma breve caraterização dos profissionais Ciber, a sua seleção e recrutamento, a sua formação e treino e os fatores que influenciam a sua retenção. Terminaremos este capítulo abordando o percurso metodológico que nos propomos fazer.

1.1. Base Concetual

1.1.1. O Ciberespaço

De criação humana, o ciberespaço foi elevado a domínio operacional pela Organização do Tratado do Atlântico Norte (OTAN), em 2016, pois, segundo Nunes (2012, p. 114), "este espaço virtual, estruturado com base numa rede de redes" é um ambiente em si mesmo com uma componente tecnológica e humana. Não tem fronteiras físicas, é transversal e influencia as operações militares em todos os domínios (figura 1), e tem de ser protegido da mesma forma que os espaços terrestre, marítimo e aéreo (Welch, 2011).

Figura 1 - Relação entre os domínios Operacionais

Fonte: (Neves, 2015, p. 17)

De salientar que no documento que contém as orientações políticas, do Ministro da Defesa Nacional (MDN), que deram início ao novo Ciclo de Planeamento de Defesa Militar, é considerado "que hoje é, porventura, muito mais significativa a ameaça ao «território» virtual, pelo número de ataques efetuados por via cibernética, constituindo os ciberataques a infraestruturas críticas de um Estado uma das mais graves ameaças à sua segurança" (MDN, 2018a, p. 11678).

1.1.2. Segurança da informação

Tradicionalmente, a defesa do ciberespaço é designada INFOSEC *(Information Security*) e, em Portugal, toma a designação de SI de natureza reativa e estática (IDN,

2013, p. 11). Sendo objetivo da SI preservar a continuidade da atividade e minimizar o impacto dos incidentes de segurança através da sua limitação (Solms e Niekerk, 2013, p. 98).

A capacidade de resposta a incidentes informáticos está nas mãos das Equipas de Resposta a Emergências Informáticas, designadas de *Computer Emergency Response Team* (CERT). Após a Cimeira de Istambul (2004), a OTAN implantou uma "capacidade semelhante a um CERT, denominando-a como CIRC ou NATO CIRC (NCIRC) (IDN, 2013, p. 31).

O EMGFA e os ramos dispõem de núcleos CIRC, que garantem a capacidade de resposta a incidentes de segurança e podem ser dados em reforço do CCD. Dispõem de uma estrutura com capacidade de resposta aos requisitos definidos pelo EMGFA para a estrutura CIRC e, quando empregues operacionalmente, integram a estrutura do CCD (Silva, 2018)

1.1.3. Ciberdefesa

As medidas de SI, perante a natureza dinâmica do ciberespaço e o crescimento das ciberameaças, são insuficientes para proporcionar um nível de proteção desejado, tendo surgido o conceito de CD, que possibilita não só defender mas, se necessário, neutralizar o atacante, através de ações de exploração e de ataque (IDN, 2013, p. 36).

As atividades de CD na doutrina americana são designadas de *Computer Network Operations* (CNO), subdividindo-se em operações ofensivas, defensivas e exploratórias (AJP-3.10, 2009, pp. 1-11).

1.1.4. Cibersegurança

A CS tem um alcance mais amplo porque abrange a SI, a segurança das Tecnologias da Informação e Comunicação, e a combinação das duas. A CS ainda inclui a dimensão humana nas suas operações, diferenciando-se assim da SI. A CS não é apenas a proteção do ciberespaço em si, mas também a proteção daqueles que o utilizam e que, por via dessa utilização, os seus ativos possam ser alcançados através do ciberespaço (Solms e Niekerk, 2013, p. 101).

O conceito de CS é abrangente e a atividade de CD concorre e contribui para a alcançar a segurança no domínio cibernético e assim como existe uma estreita ligação entre a Segurança e a DN, também a CS se revela indissociável da CD. A edificação da capacidade de CD torna possível garantir a CS em toda a sua plenitude (Nunes, 2012, p. 119).

1.2. Gestão de Recursos Humanos

Não há nenhuma estrutura que consiga operar devidamente sem os respetivos cérebros humanos. Nesta ótica, os indivíduos são encarados como um investimento e não como um custo (Neves, 2002, pp. 10, 11). Seguiremos abordando os aspetos relativos à GRH, caraterizando os profissionais Ciber, a sua seleção e recrutamento, formação e treino e retenção.

1.2.1. Caraterísticas de um profissional Ciber

O surgimento de novas tecnologias nos postos de trabalho veio provocar alterações substanciais nas exigências do fator humano" (Ribeiro, 2002, p. 267). Os profissionais Ciber por norma são apaixonados por tecnologia, nativos digitais, *hackers* criativos, inteligentes, inovadores e sedentos de conhecimento (Conti e Easterly, 2010, p. 5)

Têm uma predisposição muito acentuada para a aprendizagem e o treino faz parte da sua vida. Por outro lado, o seu conhecimento e a base das suas competências requerem uma atualização permanente (Andress e Winterfeld, 2011, p. 63).

Um estudo que examinou o capital humano Ciber da FA dos EUA, relativamente ao fator idade, refere a importância que tem de ser dada à "Geração Y" ou dos *Millennials*. Estes indivíduos, que nasceram entre 1981 e 2000, são os primeiros nativos digitais, nunca conheceram o mundo sem computadores. Segundo Bruce Tulgan (s.d., cit. por Yannakogeorgos e Geis II, 2016, p. 78), os *Millennials*, como candidatos tipo ao ingresso nas fileiras das FFAA, merecem uma abordagem diferenciada de acordo com as suas caraterísticas, sendo este o único caminho para os atrair e os manter na instituição militar (Yannakogeorgos e Geis II, 2016, pp. 77, 79).

1.2.2. Seleção e Recrutamento

A proliferação das ameaças Ciber e a chegada do ciberespaço como o novo domínio da guerra, fez crescer, por parte do setor privado e das instituições governamentais, a procura de pessoas com competências na área da CD e da SI. No processo do recrutamento, os militares têm duas opções válidas, ou recrutar internamente, convertendo militares de outras armas ou serviços, ou recrutar externamente, procurando talentos oriundos fora do meio militar. Ambas as soluções têm vantagens e desvantagens, pelo que, uma solução intermédia com recurso ao recrutamento misto, do interior e do exterior da organização, é mais equilibrada (Ribeiro, 2002, pp. 278-279).

É necessário chegar às comunidades técnicas, chamar a atenção dos mais jovens, os talentos Ciber do futuro e até considerar o recrutamento de *hackers*, não no sentido

pejorativo do termo mas dos seus conhecimentos. Outra solução passa pela contratação de civis para desempenharem funções técnicas (Nunes, Santos e Jesus, 2018).

1.2.3. Formação e Treino

A formação e o treino, enquanto funções da GRH, são um instrumento indispensável para atingir os objetivos de qualquer estratégia organizacional, criando um impacto positivo no desenvolvimento das competências individuais e na performance global da instituição (Ceitil, 2002, p. 327 e 355).

Para além da formação inicial de base, é crucial que estes RH se mantenham atualizados a par com a evolução tecnológica. É essencial a frequência de cursos de especialização, formações de atualização, de seminários e participação em exercícios operacionais (Kilaz Onder e Yanik, 2014, p. 123).

Um estudo sobre a CS elaborado por Evans e Reeder (2010, p. 5) lançou uma visão para a formação Ciber e o percurso de carreira (figura 2). Este percurso compreende quatro níveis, diretamente relacionados com os blocos educacionais construídos cumulativamente. Os peritos com alto nível de conhecimento e de capacidade, devido à sua grande experiência, devem assumir a função de líderes.

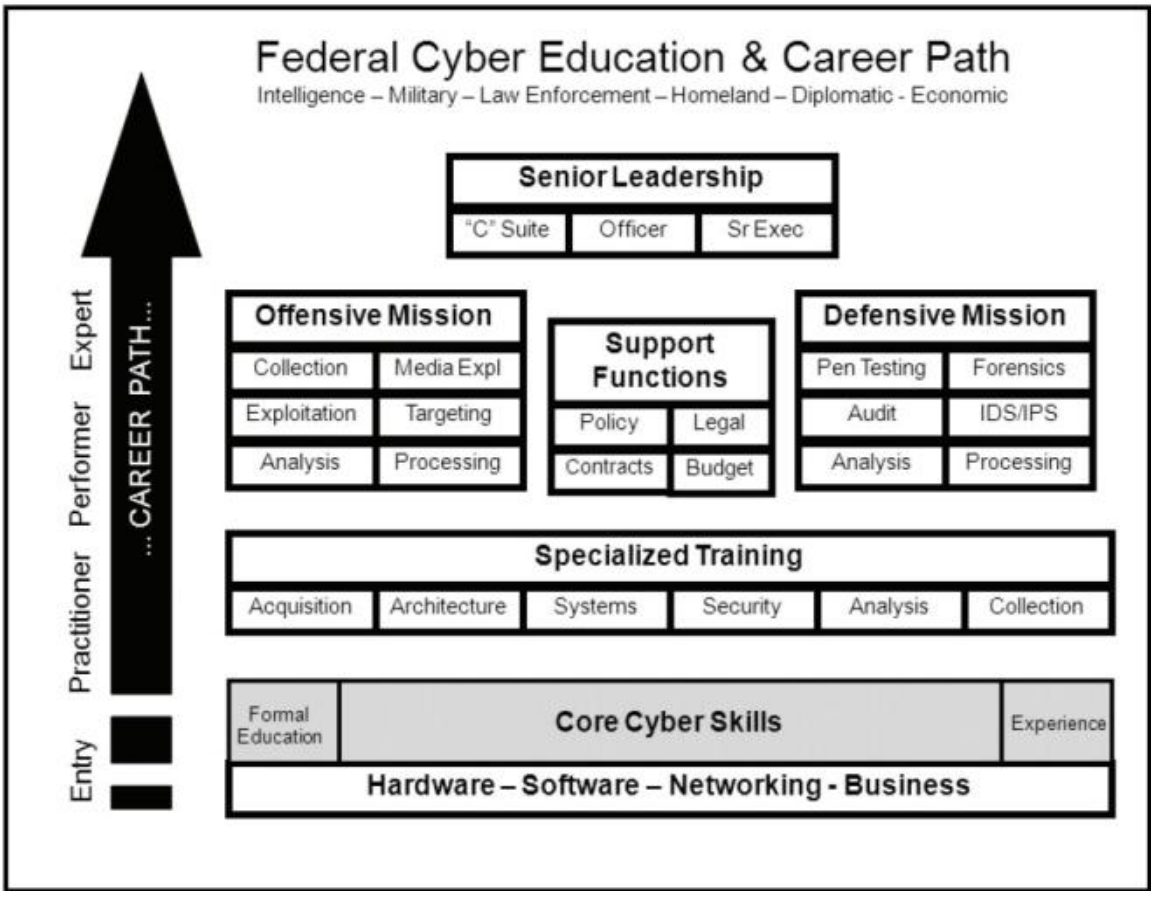

Figura 2 - Percurso de Carreira e de formação Ciber

Fonte: (Evans e Reeder, 2010, p. 5)

1.2.4. Retenção

Recrutar as pessoas indicadas para as forças Ciber é um bom início, mas mantê-las nestas equipas, representa um esforço significativo dos responsáveis pela sua gestão. Os motivos para a sua permanência podem ser variados, mas segundo Conti e Easterly (2010, pp. 9-10), a oportunidade de desenvolvimento profissional, de progressão na carreira, uma cultura Ciber apropriada e um estilo de gestão próprio, são essenciais.

1.2.4.1. Carreira Ciber

No âmbito do Estatuto dos Militares das Forças Armadas (EMFAR) (CM, 2015a, p. 3205), a "carreira militar é o conjunto hierarquizado de postos, […] a que corresponde o desempenho de cargos e o exercício de funções diferenciadas entre si", associadas a um QE, definido pelo EMFAR como o "conjunto de lugares distribuídos por categorias e postos segundo a mesma formação inicial" (CM, 2015a, pp. 3225-3226).

No que se refere à gestão da carreira, os autores Evans, et al. (2010, cit. por Kilaz, Onder e Yanik, 2014, p. 121), explicam a crise de pessoal e a falta de trabalhadores Ciber, pela insegurança criada pela inexistência de uma carreira profissional, promoções baseadas no mérito e por não se premiar e reter os que evidenciem no posto de trabalho, alto nível de competência técnica.

1.2.4.2. Remuneração

A progressão na carreira deve corresponder a um nível remuneratório competitivo e em crescendo, pois, segundo Fernandes (2002, p. 143), nas organizações que têm níveis salariais mais elevados, verificam-se taxas mais baixas de rotatividade e um maior número de indivíduos a candidatar-se a essas empresas. Também, Lawler III (1990, cit. por Fernandes, 2002, p. 413) refere que "o impacto mais óbvio do nível de compensação percebido pelos empregados é a atração, ou retenção respetiva".

1.2.4.3. Cultura Ciber

Quanto à cultura Ciber, há a referir que a perceção da comunidade técnica acerca dos militares é de uma forma geral negativa. Daqui a necessidade de construir uma cultura cibernética atraente, que valorize e respeite o conhecimento técnico, a diversidade de valores, (Conti e Easterly, 2010, p. 3). Por outro lado, Franz (2011, pp. 93-94) aponta a necessidade de implementação de uma cultura de guerra ofensiva Ciber. Primeiro, porque a maioria destes elementos foram convertidos das transmissões ou de outros ramos e tendem a focar-se em manter as comunicações a funcionar e, em segundo, porque estes profissionais têm de estar mais familiarizados com as ameaças Ciber e têm de desenvolver ataques sobre elas e têm de ser mais proactivos e menos reativos.

1.2.4.4. Gestão e Liderança Ciber

As caraterísticas das forças Ciber requerem uma gestão diferenciada, que potencie a sua retenção. É esperado que estas pessoas pensem "fora da caixa", sejam criativas e inovadoras, pelo que, sujeitá-las a uma gestão apertada, é contraproducente. Estes profissionais merecem ter líderes à altura, igualmente tecnológicos que compreendam e apreciem as suas realizações, que fortaleçam as soluções criativas para os problemas, os esforços individuais, encorajem o pensamento inovador e que saibam explorar o sucesso alcançado, potenciando a coesão da equipa (Conti e Easterly, 2010, pp. 5-6).

1.3. Resumo da metodologia

Pretende-se realizar a investigação de acordo com as Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (Santos e Lima, 2016) e conforme os regulamentos em vigor no IUM.

A estratégia de investigação a usar será qualitativa, uma vez que procuraremos a sua relação com o mundo real, ou seja, através da situação dos RH afetos à CD e SI e das abordagens e soluções adotadas por outros países, procuraremos alcançar um entendimento mais profundo do nosso objeto do estudo (Santos e Lima, 2016, pp. 29-31).

O raciocínio a utilizar será essencialmente do tipo indutivo e descritivo. Se no início do estudo elaboramos um enquadramento concetual, generalista da GRH, prosseguiremos através da observação da solução adotada por Espanha, particularmente da observação do MCCD e da associação dos dados recolhidos, estabelecer generalizações e inferir uma concetualização da GRH Ciber, que permita a sua aplicação às FFAA nacionais. (Santos e Lima, 2016, p. 20). No que respeita à GRH Ciber, vamos incidir o estudo na seleção e recrutamento, formação e treino e retenção, procurando, através da associação racional destes conceitos, melhorar a retenção destes RH na função. Depois de deduzido este raciocínio lógico, pretendemos verificar a possibilidade de melhorar a gestão destes militares, através da implementação de medidas variadas.

Quanto ao desenho de pesquisa a adotar e uma vez inserido numa estratégia de investigação qualitativa, foi estabelecido o estudo de caso, pois permite compreender o objeto de estudo do ponto de vista dos participantes, indo recolher contributos sobre a GRH do MCCD das FFAA espanholas (Santos e Lima, 2016, p. 39).

A recolha de dados será efetuada recorrendo à consulta de fontes documentais relacionadas com o tema, que levem à compreensão por parte do autor destes processos, e de entrevistas que permitam aprofundar as dinâmicas da GRH Ciber. As entrevistas serão

efetuadas a personalidades que, pela sua experiência, poderão contribuir para a investigação, de acordo com o painel de entrevistados, constante no Quadro 1.

1.4. Percurso e instrumentos metodológicos

O percurso de investigação será de acordo como preconizado no documento referencial de referência do IUM (Santos e Lima, 2016) e compreende as fases Exploratória, Analítica e Conclusiva. Estas fases integrarão a estratégia de investigação e desenho da pesquisa, apresentadas anteriormente.

Durante a fase exploratória, depois de escolhido e delimitado o tema, procurou-se definir o "estado da arte" recorrendo a várias leituras de livros, artigos e outros documentos relacionados com o tema, complementadas pela realização de entrevistas exploratórias a responsáveis pela GRH das FFAA, peritos em CD e CS, e comandantes ou antigos comandantes das estruturas dedicadas à CD e SI. Esta fase terminou com a apresentação do Projeto de Investigação.

Na fase analítica, que se desenvolveu de acordo com o modelo de análise (Apêndice B), prosseguimos a recolha documental e a revisão da literatura, pretendendo-se dar resposta às QD, através da caraterização e interpretação dos dados recolhidos através de leitura de bibliografia relacionada com o tema e dados resultantes das entrevistas semiestruturadas que se efetuaram. Na fase conclusiva, avaliamos e discutimos os resultados, respondemos às QD através das quais obtemos resposta à QC, concretizando os OE e o OG da investigação. Apresentamos as conclusões, a nossa contribuição para o conhecimento, qual o modelo de GRH Ciber, que mais contribui para o funcionamento operacional do CCD e CIRC das FFAA.

2. Impacto da Gestão de Recursos Humanos na capacidade de Ciberdefesa

> "*O domínio ciberdefesa é hoje um teatro de operações, é um quarto domínio operacional, então vai ser preciso que Portugal, com a capacidade que temos, aposte em tornar-se, não digo numa potência, mas tornar-se num país forte, respeitado e credível nessa dimensão `ciber´*"
>
> Azeredo Lopes (MDN, 2018b)

Neste capítulo, após enquadrar a criação do CCD, analisaremos o atual impacto que a GRH tem na capacidade de CD, recorrendo à metodologia DOTMLPI-I utilizada pela OTAN, para a edificação de capacidades operacionais, aplicando-a à atual capacidade do CCD. Os vetores da capacidade, que dentro desta metodologia tocam os RH e a sua formação, serão analisados de forma mais aprofundada. O CCD é a estrutura centralizadora de toda a capacidade de CD das FFAA, uma vez que operacionalmente recebe os recursos dos núcleos CIRC dos ramos.

2.1. Criação do Centro de Ciberdefesa

A Cimeira de 2016 da OTAN, em Varsóvia, onde todos os aliados assumiram fortalecer as capacidades de CS e CD nos termos do "*Cyber Defence Pledge*", veio reforçar os compromissos internacionais assumidos por Portugal (NATO, 2016).

Após reforma da "Defesa 2020" (CM, 2013b) e posterior Orientação Política para a Ciberdefesa (OPC) (MDN, 2013b), o EMGFA, em dezembro de 2013, elaborou um Plano para a Edificação da Capacidade de Ciberdefesa Nacional (PECCN), onde identificou os "diversos vetores de desenvolvimento da capacidade de Ciberdefesa nacional, nomeadamente a missão, a estrutura orgânica e os recursos necessários para a sua edificação", em articulação com os ramos e serviços centrais do MDN, com o objetivo de criar o CCD na dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA) (DICSI/EMGFA, 2013, p. 5).

Através da LO do EMGFA (CM, 2014) é criado o CCD integrado na Direção de Comunicações e Sistemas de Informação (DIRCSI) (figura 3), tendo alcançado a *Initial Operational Capability* (IOC) em junho de 2016. O Decreto Regulamentar 13/2015 (CM, 2015b), onde é estabelecida a organização e competências das estruturas principais do EMGFA, elenca, no seu Art.º 45º (Anexo A), um conjunto de competências para o CCD no âmbito da CD nacional e da CS setorial, designadamente a responsabilidade pela condução

de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas (CM, 2015b, p. 5287).

Figura 3 - Estrutura da DIRCSI

Fonte: (DICSI/EMGFA, 2013, pp. 15-18)

De acordo com o PECCN, o CCD deveria ter uma área responsável pela direção e coordenação, uma área dedicada às operações militares no ciberespaço e uma outra área dedicada ao conhecimento concreto das ameaças (DICSI/EMGFA, 2013, p. 18). Para efeitos de condução de operações militares no ciberespaço, o CCD fica sob Comando Operacional do CEMGFA e, quanto ao exercício das suas atribuições de natureza permanente, o CCD integra-se na estrutura da DIRCSI do EMGFA (DICSI/EMGFA, 2013, p. 17).

Apesar do CCD, segundo o PECCN, dever atuar como ponto central na estratégia de CD e na condução de operações no ciberespaço, segundo Camelo dos Santos (2017, p. 33) "todas as atividades se centraram na esfera da ciberdefesa enquanto promotora da segurança da informação, traduzida na edificação de uma estrutura central tipo *computer emergency response team* (CERT) conectada a três CIRC nos ramos." Recebe os eventos de segurança dos ramos, contribui para o desenvolvimento de elementos doutrinários, definição de procedimentos e estratégias conjuntas e coordenação de exercícios (DICSI/EMGFA, 2013, pp. 12, 13).

Segundo Monteiro (2017, p.C1 cit. por Santos, 2017, p. 20) é premente "fazer evoluir o atual CCD para uma estrutura de comando para a componente cibernética", prevendo Nunes (2018) que "nos próximos anos temos que ter pelo menos um comando semelhante ao Comando de Componente das Operações Especiais". Neste aspeto, também Camelo dos Santos (2017, p. 61) defende a necessidade de "edificação de uma estrutura de ciberdefesa

assente num comando de componente, à reformulação dos EM por incorporação de valências de ciberdefesa nas células J6/G6 e à criação de equipas táticas de ciberdefesa, incorporando as especificidades dos ramos e constituindo um todo coerente enquanto força conjunta de ciberdefesa."

Atendendo ao novo ciclo de Planeamento de Defesa Militar, iniciado pelo MDN (2018a) e da Diretiva Estratégica do EMGFA 2018/2021 (Anexo B), da qual se retira a intenção do CEMGFA de dinamizar a edificação da capacidade de CD nacional, prevê-se que a curto prazo haja alterações à capacidade de CD nacional (Ribeiro, 2018a, p. 28).

2.2. Análise da capacidade de Ciberdefesa do CCD

2.2.1. Doutrina

Em caso de ataque deliberado a Portugal e que seja necessário ativar a resposta militar, os mecanismos legais de resposta não são específicos para a CD, pois são mecanismos incapazes de lidar, por exemplo, com o tempo de reação a ataques no ciberespaço (figura 4). Segundo Camelo dos Santos "urge adaptar o *modus operandi* da tomada da decisão operacional", que o anterior CEMGFA (Monteiro, 2017, cit. por Santos, 2017, p.32) considerava importante: a " criação de um quadro de referência orientado para a sistematização dos procedimentos de ação e reação a eventos que venham ocorrer".

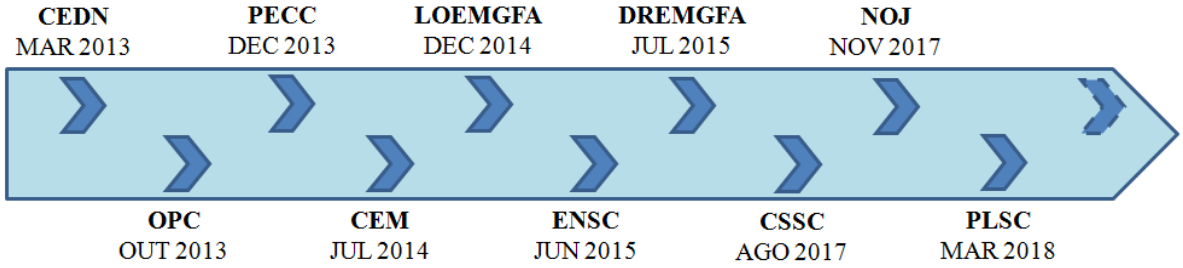

Figura 4 - Enquadramento legal da Ciberdefesa

Fonte: (autor, 2018)

A Estratégia Nacional de Segurança do Ciberespaço (ENSC) (CM, 2015c), que se encontra em revisão[3], é o documento enquadrador da segurança das redes e da informação, mas não aborda a defesa nesta perspetiva. Concretamente existe a OPC, no entanto, falta uma "Estratégia Nacional para a Ciberdefesa" e esta lacuna de enquadramento, reduz a eficácia da capacidade, embora esteja constituído um grupo de trabalho com vista a apresentar esta estratégia (Nunes, 2018), prevista recentemente na Diretiva Estratégica do EMGFA 2018/2021 (Ribeiro, 2018a, p. 28).

[3] Esta revisão surge da constituição do Conselho Superior de Segurança do Ciberespaço, que tem por missão assegurar a coordenação político-estratégica para a segurança do ciberespaço, o controlo da execução da ENSC e da respetiva revisão. Nos termos da RCM n.º115/2017 de 24 de agosto, publicado no DR N.º 163 — 24 de agosto de 2017 (CM, 2017, p. 5036).

2.2.2. Organização

A organização interna, está relacionada com a forma como as pessoas constituem as equipas, executando cada uma delas funções diversas. Estas equipas devem funcionar de forma coordenada, com processos de resposta adquiridos que decorram do seu treino (Neves e Correia, 2016, p. 9).

No âmbito da CS, se pensarmos no CCD como um *Security Operations Center* (SOC), deverão constar equipas que cubram todas as funções (Torres, 2015, p. 4), mas as "competências do foro jurídico, indispensáveis na condução de operações neste domínio", têm de vir dos ramos, no entanto, estes elementos não dispõem de preparação jurídica específica e muito menos dedicação funcional nesta área. Também, ao nível da componente estratégica, deveria haver um incremento de oficiais de Estado-Maior, na medida em que as solicitações são cada vez maiores (Pires, 2018).

Naturalmente que o reduzido número de elementos do CCD, do ponto de vista de organização interna, compromete e afeta negativamente a constituição das equipas, a sua manutenção, treino, qualificações associadas e procedimentos, influenciando decisivamente a sua capacidade de resposta a incidentes.

2.2.3. Treino

Sem treino, as equipas referidas anteriormente, não adquirem os conhecimentos nem os processos necessários para responderem cabalmente a incidentes.

A ENSC evidencia que o sucesso da segurança do ciberespaço passa pela promoção de uma cultura de segurança que proporcione a todos o conhecimento e, também, que o país se dote de RH qualificados para lidar com os complexos desafios da segurança do ciberespaço (CM, 2015c, p. 3741).

Este percurso de aprendizagem é moroso, não tem soluções alternativas, e as capacidades técnicas resultam de um conjunto de valências que se vão gerando ao longo do tempo e funcionando por sedimentação. É imperioso que o plano de implementação desta capacidade militar contemple um plano de formação que possibilite a multiplicação dos especialistas, permita alocar mais gente nas funções, para dar corpo à estrutura e permitir o crescimento da capacidade de CD (Nunes, 2018).

Portugal é líder de um dos *smart defense projects*, no âmbito da educação e treino "é o país de charneira em termos de ligação entre a UE e a NATO, na área de educação e treino de CD" (Nunes, 2018) e, desde 2013, lidera o *Multinational Cyber Defense Education and Training Project* (MN CD E&T). Prepara-se, igualmente, para receber a Escola de Comunicações e Sistemas de Informação e um Centro de Treino Ciber, ambos

da OTAN e, paralelamente, será responsável pela gestão da Plataforma Centralizada da União Europeia (UE) de Treino e Exercícios de CS. Embora sejam responsabilidades assumidas internacionalmente, estas iniciativas, para além de representarem condições excecionais para formar e treinar os RH Ciber (Monteiro, 2017), colocam-nos no ponto central desta rede integrada entre a UE e OTAN, pelo que merecem ser potenciadas ou perdemos o seu valor estratégico.

O treino é fundamental para a aquisição de processos de atuação. Permite avaliar e desenvolver a doutrina, identificar lacunas e gerar confiança e sentimento de comunidade entre todos os intervenientes da comunidade Ciber. Neste âmbito, o Exército tem organizado anualmente, desde 2012, o exercício *Ciber Perseu* e, a nível internacional, destaca-se a participação no exercício anual de CD, denominado por *Cyber Coalition*, da OTAN, com o propósito de treinar a coordenação entre nações (Assunção, 2018).

Este ano, o Centro Nacional de Cibersegurança (CNCS) irá coordenar o primeiro exercício nacional de CS 2018, o ExNCS, agendado para maio de 2018. Também as FFAA irão realizar, no último trimestre do ano, um exercício, o *Cyber FA Lead* e, também pela primeira vez, na qualidade de participante, no exercício na OTAN *Locked-shields*, após assinatura da nota de adesão[4] ao Centro de Excelência para a Ciberdefesa Cooperativa da OTAN, o *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) (Assunção, 2018).

2.2.4. Material

O CCD como órgão coordenador é responsável pelos estudos e processos de aquisição do material necessário para suportar e equipar as equipas Ciber, resultando uniformidade de equipamentos e capacidades entre o CCD e as estruturas CIRC (Silva, 2018).

2.2.5. Liderança

A Liderança está diretamente relacionada com a formação e surge no topo da carreira Ciber, garantindo-se assim que as chefias possuam as competências profissionais necessárias e que estão preparados para uma abordagem profissional da operação (Neves e Correia, 2016, p. 10). O reduzidíssimo número de RH, as necessidades de formação, desperdício de recursos em tarefas repetidas e a dificuldade de atribuição de funções tendo em conta a experiência, a motivação e a especialização de cada elemento, são o maior desafio à liderança (Costa, 2017, p. 13).

[4] A adesão de Portugal ao CCDCOE da OTAN foi autorizada em novembro de 2017 pelo MDN (Despacho n.º 9762/2017 de 19 de outubro do MDN), apenas formalizada no dia 24 de abril de 2018, aquando da primeira participação das FFAA portuguesas, no exercício de CD internacional *Locked Shields* (Agência Lusa, 2018).

2.2.6. Pessoal

Este vetor é o mais importante para a operacionalização da capacidade. O CCD tem um Quadro Orgânico (QO) diminuto, não tem colaboradores civis e conta com dez militares (tabela 1), embora neste momento, efetivamente apenas disponha de nove (Jesus, 2018).

Tabela 1 – Quadro orgânico do CCD

CMG/COR	CFR/CTEN/TC/MAJ	1TEN/CAP	SCH/SAJ	TOTAL
1	3	3	3	10

Fonte: Adaptado de (DICSI/EMGFA, 2013, p. 18)

A chefia do CCD é atribuída à vez a cada um dos ramos, por um período de dois a três anos. Da mesma forma, as posições de oficiais superiores, capitães e sargentos são preenchidas por cada um dos ramos, com partilha tripartida, competindo-lhes preencher uma vaga em cada uma das posições (Santos, 2018). Quanto à diversidade de postos na categoria de oficiais, esta foi projetada com a intenção de permitir a progressão na carreira aos especialistas. Permite que os mais novos, acabados de formar pelas universidades, com conhecimentos sobre os novos sistemas operativos, novo *hardware*, novo *software* e o seu funcionamento, possam dar o seu contributo ao CCD e ao mesmo tempo completem as suas competências (Nunes, 2018). A integração dos sargentos resulta da necessidade funcional de efetuar registos, manter a carta de situação do ciberespaço, efetuar configurações de sistemas e apoiar o trabalho administrativo (DICSI/EMGFA, 2013, p. 18).

Embora doutrinariamente ainda não esteja definido um conceito operacional que exija, por exemplo, o funcionamento do CCD em permanência (24/7/365), como evidenciado pelo Diretor da DIRCSI (Pires, 2018), segundo a OPC, "as FFAA devem dispor de uma capacidade de recolha e análise de informações no ciberespaço, capaz de permitir, em tempo, uma resposta eficaz", o que com o atual QO, parece de todo impossível.

É um número de facto insuficiente, não abrange todas as vertentes, algo visível na realização de exercícios, para os quais o CCD acolhe os meios dos ramos, podendo chegar a 30 elementos. Um aumento de pessoal na ordem dos 300%, e este conceito de *Augmentees* ao CCD encontra-se institucionalizado (Jesus, 2018).

O reduzido QO, associado à rotatividade dos militares, por via das comissões de serviço que, na melhor das hipóteses, garantem a permanência por um período máximo de cinco anos, a necessidade de progressão na carreira militar e o tempo de formação

associado, dificultam a manutenção das equipas e das qualificações associadas (Costa, 2017, p. 11).

2.2.6.1. Seleção e colocação de militares no CCD

A alimentação do CCD com RH foi idealizada recorrendo aos ramos. Foi a forma mais rápida para o fazer face às necessidades desta nova estrutura, sendo, de forma geral, o que acontece em toda a estrutura do EMGFA, nos termos do Art.º 49 º da sua LO. Não se vislumbrando outra, esta solução apresenta desvantagens, pois estes elementos têm maior apetência para ações defensivas; necessitam de treino e preparação; e não representam efetivamente um ganho, porque não estão a engrossar as fileiras (Kilaz Onder e Yanik, 2014, p. 118). Adicionalmente, com mais uma estrutura a guarnecer de militares, os ramos perdem militares por determinado tempo, o que, segundo Nunes (2018), não é uma boa solução porque estamos a pulverizar os parcos recursos existentes, em vez de "concentrar para multiplicar". Pode-se, ainda, inferir que os ramos, na tentativa de preservarem os seus melhores recursos, não cedam os militares melhor preparados.

2.2.6.2. Retenção no CCD

Os militares indicados para exercerem funções no CCD não gozam de nenhuma exceção relativamente ao tempo de permanência no EMGFA. Efetivamente, ficam sujeitos ao regime geral de "comissão de serviço por três anos, renováveis por mais dois anos" nos termos do n.º 7 do Art.º 49 º da LO do EMGFA e, se ao fim dos três anos de permanência, os militares e as respetivas chefias entenderem que devem continuar, essa situação deve ser solicitada através de requerimento.

No entanto, a OPC refere a adequação da GRH de modo a "garantir a sua permanência em atividades relacionadas com esta temática por períodos não inferiores a cinco anos" (MDN, 2013b, p. 31978), referindo Nunes (2018) que os militares deveriam permanecer por um período mínimo de oito anos.

Logo à partida o modelo de comissão de serviço é castrador relativamente à retenção destes elementos, porque está limitada pela perspetiva da rotatividade. Por outro lado, ela é fundamental, porque têm de ser garantidas as condições especiais de promoção, de acordo com o art.º 63º, as mesmas condições e oportunidades de progressão de carreira, de acordo com o art.º 123º, e garantidas as condições de desenvolvimento da carreira, de acordo com a alínea c) do n.º 1 do art.º 132º, todos do EMFAR. Passados sensivelmente três anos e meio após a criação do CCD, os militares permanecem no CCD, perspetivando-se que cumpram os cinco afetos a este órgão.

A opção por uma carreira horizontal, prevista no Art.º 125º do EMFAR, progredindo em posições remuneratórias, poderá ser uma solução que garanta maior permanência dos militares nestas funções, mas é uma situação que ainda não foi regulada em diploma próprio. Outra situação prende-se com o assédio do mercado de trabalho, sobre os melhores elementos, oferecendo níveis salariais quatro vezes superiores aos auferidos nas FFAA. Três militares que exerciam funções nas estruturas ligadas à CD e SI, solicitaram sair das FFAA, estando a trabalhar em empresas civis (Silva, 2018).

2.2.7. Infraestruturas

Este vetor prende-se com a existência de instalações adequadas à preparação e condução das operações. No caso do CCD, optou-se por o instalar no edifício do EMGFA, que, não sendo uma estrutura criada de raiz para o efeito, serve, apesar das suas limitações e, ainda, garante, para além de requisitos técnicos de segurança, as necessárias condições logísticas, se, por motivos doutrinários e operacionais, ou de crise, for exigido o seu funcionamento em permanência (Pires, 2018).

2.2.8. Interoperabilidade

De louvar a criação, em agosto último, do Conselho Superior de Segurança do Ciberespaço, que tem a responsabilidade de assegurar a coordenação político-estratégica para a segurança do ciberespaço, distribuída por diferentes entidades com missões e objetivos diversos (CM, 2017, p. 5036).

Segundo Neves (2015, pp. 95-96), o fator interoperabilidade (figura 5) é fundamental para que, perante a natureza complexa e difusa da ciberameaça e o risco de um ataque em larga escala, a resposta entre os diversos atores privados e públicos, nacionais ou internacionais, seja coordenada e cooperativa.

Figura 5 - Ligações de interoperabilidade

Fonte: (Neves, 2015, p. 95)

Quantas mais forem as organizações que cooperativamente assegurem a segurança do ciberespaço, mais seguro ele se torna. Como se vê representado na figura 5, os CIRC das FFAA partilham a informação com o CCD, que por sua vez a partilha com o CNCS, a nível nacional, e com o NCIRC, a nível internacional, no quadro das organizações militares. Esta responsabilidade assenta em três patamares. O primeiro, entre os CIRC e o EMGFA, o segundo, entre o EMGFA e as organizações nacionais e, um terceiro, entre o EMGFA e a OTAN. Segundo Camelo dos Santos (2017, p. 30), na "esfera da cibersegurança, […] constata-se a realização de um trabalho relevante ao nível das FA, que se encontra em adiantado grau de execução por via da implementação de ferramentas operativas num cada vez maior número de órgãos da DN".

2.3. Síntese conclusiva

Através da avaliação DOTMLPI-I evidenciamos o papel determinante que os RH têm nesta capacidade, porque, dos oitos vetores analisados, quatro são influenciados diretamente pelos RH. As pessoas constituem o elemento decisivo para identificar, defender e, se necessário, atacar as fontes das ameaças Ciber.

Se considerarmos o CCD como uma estrutura dedicada apenas à SI e que os militares lá colocados aquando da sua criação ainda se mantêm em funções, poderíamos dizer que o impacto da atual GRH nesta capacidade é nulo, no entanto o CCD, de acordo com a legislação enquadradora (Anexo A), foi criado para desenvolver operações de CD, pelo que, em resposta à QD 1, conclui-se que o impacto da atual GRH na capacidade operacional de CD e SI é negativo (Apêndice C).

Constatamos: que as pessoas influenciam a Organização, porque só com um efetivo adequado permitem constituir as equipas; que o Treino é indispensável para garantir uma resposta à altura das ameaças, onde se inclui a formação; que a Liderança constitui o topo da carreira a atingir, através da formação e experiência; e que o Pessoal é a "verdadeira capacidade e o seu centro de gravidade" (Nunes, 2018). Constatações que colocam às FFAA "o desafio adicional de recrutar e reter o pessoal mais qualificado, capaz de integrar os requisitos inicialmente estabelecidos e, proactivamente, promover a inovação e a evolução constante, tanto do nível de conhecimento, competências e técnicas, como da própria doutrina de emprego operacional das capacidades" (Santos, 2017, p. 21).

O reduzido número de elementos e a rotatividade desses elementos, consequência da comissão de serviço e da manutenção dos direitos e das garantias de progressão de carreira, são incontornáveis e definem a GRH Ciber, em nada diferente da empregue nas FFAA em geral, que compromete esta capacidade.

Num processo natural de maturação e de evolução da SI e CD nacionais e indo ao encontro dos compromissos internacionais assumidos, o CCD, a curto prazo, tendo em conta as declarações do MDN (2018b) e a Diretiva Estratégica do CEMGFA 2018/2021, poderá evoluir para um Comando Ciber (CC), mas esta nova estrutura, padecerá dos mesmos problemas ao nível da GRH, sendo imperioso implementar melhorias.

3. Abordagem do Reino de Espanha à Ciberdefesa e Segurança da Informação

> "*Las Fuerzas Armadas están a día de hoy "extraordinariamente tecnificadas" y necesitan "imperiosamente utilizar el ciberespacio", tanto que si pierden el acceso al mismo, "retrocederían 60 años*".
>
> López de Medina (MCCD, 2017)

Neste capítulo iremos apresentar o caso do MCCD, recorrendo à metodologia DOTMLPI-I, conforme efetuado para o CCD, que nos permitirá efetuar um estudo comparativo. Trata-se de um CC de menores dimensão, recente, de um país da OTAN com boas relações com Portugal e, de todos, o que, por diversas circunstâncias, se revelou o mais acessível para estudar.

Outras abordagens poderiam ter sido estudadas de forma mais profunda, como a dos EUA, porque doutrinariamente são considerados os mais avançados; a do Brasil, que atribuiu ao Exército Brasileiro (EB) a responsabilidade de criação, sustentação e prestação deste serviço aos outros ramos; ou a da Alemanha, que avançou para a criação de mais um ramo nas suas FFAA (Apêndice A).

3.1. Criação do MCCD

A *Estrategia de Ciberseguridad Nacional*, de 2013, em estreita articulação e reforçada pela *Estrategia de Seguridad Nacional*, de 2017, elevaram a CS ao topo das prioridades para a segurança nacional em Espanha. O *Consejo de Seguridad Nacional* constitui o núcleo deste sistema, desenvolvendo a estrutura ao nível político em articulação com a estrutura ao nível executivo (Cendoya, 2016, p. 8 a 10).

O MCCD é um órgão da estrutura operacional que traduz a assunção do ciberespaço como um domínio operacional pelo Estado espanhol (Santos, 2017, p. 46). É subordinado ao Chefe do Estado-maior da Defesa, responsável pelo planeamento e execução das ações relativas à CD nas redes e sistemas de informação e telecomunicações do Ministério da Defesa e outras que possam ser atribuídas, e contribui para a resposta adequada no ciberespaço perante ameaças e agressões que possam afetar a DN (EM da Defensa, 2018).

O MCCD (figura 6) foi criado em 19 de fevereiro de 2013 por ordem ministerial e alcançou a sua IOC no final de setembro, apenas sete meses depois. Constitui o quarto pilar, juntamente com os comandos da Vigilância Marítima, Defesa Aérea e Operações Especiais, da força conjunta das FFAA espanholas (Onemagazine, 2014).

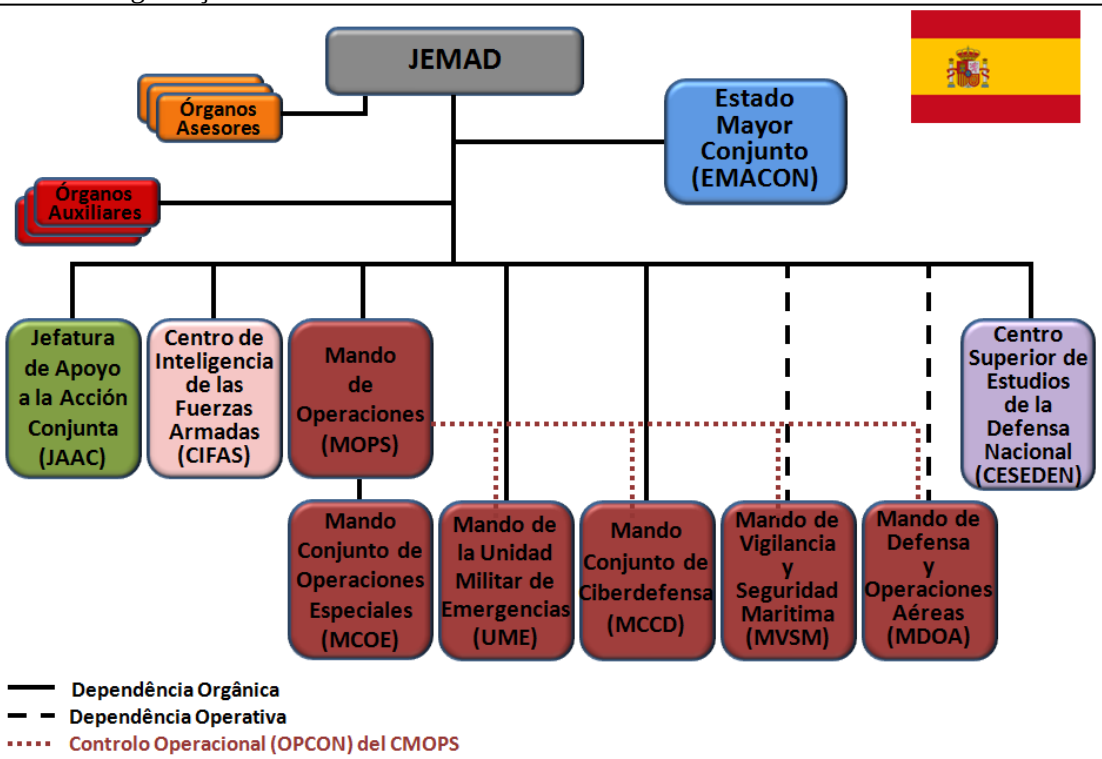

Figura 6 - Organograma do EMAD

Fonte: (EMAD, 2018)

3.2. Análise

De seguida, seguindo a metodologia do capítulo anterior, vamos analisar a capacidade de CD e SI do MCCD.

3.2.1. Doutrina

Segundo declarações do Comandante do MCCD, para além da *Estrategia de Ciberseguridad Nacional*, houve necessidade de escrever os procedimentos e doutrina, porque estes não existiam, procurando incluir a CD nas operações militares, combinando-a com os demais elementos (Ruiz, 2016).

O MCCD tem três capacidades: defesa, exploração e ataque. A primeira, refere-se à defesa dos sistemas de informação perante um ataque e a sua recuperação em caso de falha, ou inutilização total ou parcial. A capacidade de exploração está relacionada com atividades de recolha de informações, o que implica entrar dentro dos sistemas adversários e investigar o que existe neles. Por último, a capacidade de resposta ou de ataque, serve para neutralizar total ou parcialmente os sistemas adversários (Arce, 2017).

3.2.2. Organização

A estrutura do MCCD é uma organização que existe em Espanha e em muitos outros países da OTAN. Conta com um Estado-maior, um chefe de operações e um chefe de apoio e serviços. A secção de operações é a que dispõe de mais pessoal, com um grupo

destinado à defesa e, outro grupo, destinado á exploração e resposta. Também conta com um grupo técnico, que está relacionado com as empresas e as Universidades, para incorporação dos avanços tecnológicos (figura 7) (Europapress, 2013).

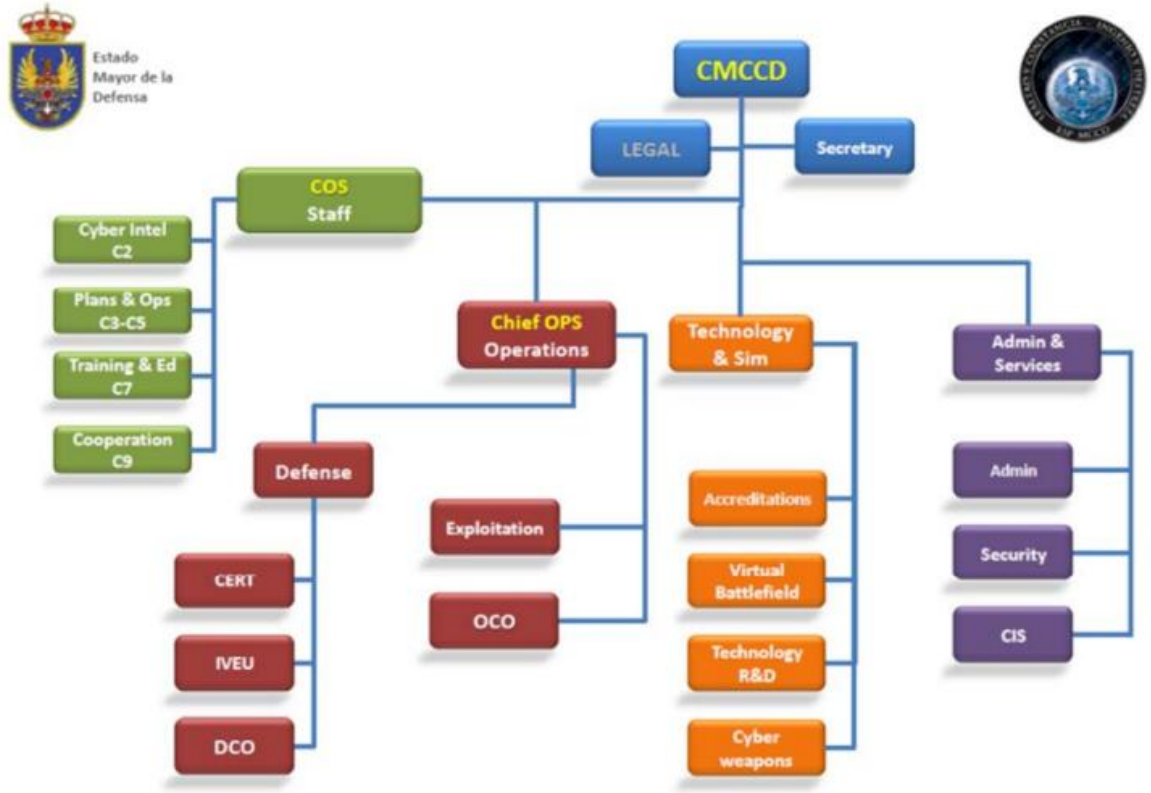

Figura 7 - Estrutura do MCCD

Fonte: (Santos, 2017, p. 46)

Embora não nos tenha sido possível chegar ao número exato de militares e civis que atualmente constituem o MCCD, atendendo que alcançou a sua IOC no final de setembro de 2013, tendo disponível cerca 50% do seu pessoal, ou seja 35 membros (Onemagazine, 2013), e que, desde essa altura, se encontra plenamente operativo com capacidade defensiva e ofensiva e de formação, fruto da estratégia implementada, estamos em crer que os seus elementos são em número superior, portanto suficientes para constituição das equipas necessárias ao funcionamento operacional do MCCD.

3.2.3. Treino

Segundo o General Medina o treino é constante "*desde que son un embrión van resolviendo todo lo que pueden*", estão em constante crescimento e aprendizagem. Como no ciberespaço não existe paz absoluta**,** há sempre atividade, o treino é permanente. Do pessoal militar, podem ser distinguidos dois grupos, os que têm experiência em sistemas de informação devido a trabalhos e funções anteriores e os que não têm (Álvaréz, 2017).

A formação, que vai dos cursos mais generalistas aos mais especializados, é repartida pelos ramos das FFAA. O curso básico é ministrado na *Escuela de Especialidades de la Armada*, o curso avançado na *Academia del Arma de Ingenieros*, e os cursos de especialidade na *Escuela de Técnicas Aeronáuticas*. Estes polos são denominados de *Centros Universitarios de la Defensa* (CUD) adstritos a cada um dos ramos (Ágreda, 2016, p. 158). Para além disso, a CD está incluída na formação base das academias militares, cursos de qualificação e na Escola Militar de estudos jurídicos e nos cursos do Centro de Estudos Superiores de Defesa (Santos, 2017, p. 48), o que nos leva concluir que o plano de edificação da capacidade, contemplou um plano de formação específica da CD.

Quanto ao treino, o MCCD participa em vários exercícios com a OTAN, que contribuem para o treino e aperfeiçoamento das habilidades dos seus membros. Dos exercícios realizados todos os anos, há dois realizados pelo NATO CCDCOE, o *Locked Shields*, realizado na primavera, em que cada nação participa com a sua equipa e outro mais amplo, o *Cyber Coalition*, em que a organização vai introduzindo diferentes eventos nas nações estas têm de reagir (Ruiz, 2016). Em 2017, uma equipa do MCCD participou no *Crossed Swords*, um exercício organizado pelo NATO CCDCOE.

A nível nacional, o MCCD participou, em 2017, num exercício planeado pela Unidade Militar de Emergências (UME), um exercício real que incorporou a vertente Ciber. Neste exercício, o MCCD ficou responsável pela Ciberdefesa do sistema de Comando e Controlo da UME. (Arce, 2017)

3.2.4. Material

O MCCD, para além de um orçamento específico ao nível do Estado-Maior da Defesa (Santos, 2017, p. 48), de acordo com as entrevistas ao seu Comandante, está equipado com todo o material necessário para executar as missões que lhe estão atribuídas (Ruiz, 2016). Relativamente a este assunto, foi possível apurar que o MCCD durante os anos de 2014 e 2015 recebeu a quantia de quatro milhões e 800 mil euros, repartidos pelos dois anos, para investimento em contratação de serviços de informática, *software* e outros materiais necessários para garantir o cumprimento da missão (Belt, 2013).

3.2.5. Liderança

Desde 03 de julho de 2013 que o MCCD é liderado pelo General de Divisão Carlos Gómez López de Medina (figura 8), Chefe deste comando conjunto. Oficial de carreira, oriundo da FA, possui vasta experiência profissional, destacando-se a sua passagem pelo Estado-Maior da FA espanhola, e tem formação na área das transmissões e guerra eletrónica e especializações em telecomunicações (EMD, 2013).

Figura 8 - General López de Medina
Fonte: (González, 2013)

Fruto do plano de formação implementado, "está em preparação um programa para adaptação das lideranças ao novo ambiente operacional" e o processo de tomada de decisão está perfeitamente definido e estratificado desde o nível político ao tático (Santos, 2017, p. 48).

3.2.6. Pessoal

Quando alcançar a sua capacidade operativa final, o MCCD contará com uma equipa de 70 elementos, das quais 49 são militares e 21 são civis contratados (Onemagazine, 2014). Segundo o EM MCCD, prevê-se um aumento escalonado e progressivo do pessoal, em função da evolução do ambiente operacional, estimando-se que possa chegar nas FFAA a um número acima dos 700 (EM MCCD, 2018).

Os militares são oriundos dos três ramos das FFAA espanholas, Marinha Exército e FA, não havendo distinção entre o pessoal do MCCD, dos que trabalham noutros domínios, não têm uma gestão diferenciada, nem mecanismos de retenção próprios (EM MCCD, 2018).

O modelo é muito recente, todavia encontra-se em fase de ajuste. Para além disso, há que ter em conta que, como foi criado num cenário orçamental muito condicionado por um orçamento restritivo, conta com questões do tipo conjuntural que estão a ser corrigidos à medida que o cenário orçamental melhora. Por outro lado, como os seus RH provêm dos ramos, que necessitam deles para as suas próprias missões, a sua captação é dificultada. Futuramente, pretendem aplicar de forma efetiva o modelo inicialmente previsto, que contempla a criação de uma especialidade fundamental de CD (EM MCCD, 2018).

3.2.6.1. Seleção e colocação de militares no MCCD

Em Espanha, as vagas para diferentes organizações, como o MCCD, são publicadas periodicamente no Boletim Oficial de Defesa e os militares dos ramos podem candidatar-se a esta organização desde que cumpram os requisitos exigidos, tais como Posto, formação em informática e nível de inglês. Quem for selecionado para exercer funções no MCCD, perde a colocação anterior e tem de permanecer pelo tempo mínimo de dois anos, não havendo tempo máximo, mas tem de manter os requisitos, como, por exemplo, o posto. São recrutados militares das três classes, oficiais, sargentos e praças, para garantir as diferentes funções de trabalho. Após cumpridos dois anos, o militar pode candidatar-se a outro lugar, no ramo ou num órgão da Defesa (EM MCCD, 2018).

Normalmente, o pessoal especializado em tecnologias da informação e nas telecomunicações é o mais apropriado para estas missões e muitos destes elementos, por iniciativa própria, já têm alguma especialização em CS que complementam quando chegam ao MCCD, havendo outros que não têm esta especialização (Ruiz, 2016).

Depois de selecionados, os elementos do MCCD recebem formação específica, tendo sido estabelecidos quatro níveis de capacitação que se alcançam superando os cursos correspondentes. Para alcançar o quarto e o último nível de capacitação, é necessário um tempo máximo de dois anos, em função dos conhecimentos iniciais de cada um (EM MCCD, 2018).

Esta política de recrutamento, aumenta substancialmente o universo de recrutamento porque incorpora militares das diferentes categorias, oficiais, sargentos e praças, que são empregues em diferentes funções, bem como aqueles que têm formação na área e os que não possuem qualquer tipo de formação específica na área, mas que depois o MCCD garante essa mesma especialização.

3.2.6.2. Retenção no MCCD

No âmbito militar, no entanto, a política de pessoal não é flexível, sendo necessário combinar necessidades com as transferências e colocações, o cumprimento das condições para dar condições de promoção, a frequência dos cursos de promoção, e outros motivos (Durán, 2010, p. 247). Ainda, não parece fazer sentido que, tanto os militares como os civis tenham de permanecer por um período mínimo de dois anos, quando a formação específica demora esse mesmo tempo.

Neste momento, decorre um plano de consciencialização das FFAA para a CD, que é essencial para afirmar a importância da estrutura desta organização, impulsionar a cultura

cibernética, como um conceito transversal que se está a incorporar no planeamento e execução das operações em todos os níveis (EM MCCD, 2018).

A perspetiva de carreira com vista à progressão destes militares, é similar ao resto do pessoal das FFAA, não auferem nenhum suplemento remuneratório, similar ao resto do pessoal das FFAA, e as possibilidades de evoluir na carreira, de aprofundar os conhecimentos, assumir cargos com maior responsabilidade, são similares ao resto das FFAA (EM MCCD, 2018).

3.2.6.3. Funcionários civis no MCCD

O pessoal civil é composto por técnicos, sendo difícil captar pessoal civil com muita experiência, pois esses são cativados por empresas privadas que oferecem vencimentos mais altos. Daí que a alternativa passa por captar indivíduos mais jovens com grande potencial com os quais se tenta produzir uma simbiose, oferecendo a oportunidade de trabalhar com tecnologia, procedimentos e outros projetos de infraestruturas. É possível garantir uma experiência completa que pode ser potenciada como experiência para o seu futuro (Ruiz, 2016). Segundo o EM do MCCD, os civis "fornecem uma visão que o pessoal militar não tem, em termos de resolução de conflitos" (EM MCCD, 2018).

A este propósito o Estado Espanhol, através da Comissão de Segurança nacional do Congresso, propôs a criação de uma Ciber reserva de *hackers*, na qual o Comandante do MCCD vê vantagens como a alta qualificação e a oportunidade para aumentar a força de forma flexível, para atuar em caso de necessidade (Piña, 2017).

3.2.7. Infraestruturas

O MCCD está instalado nas antigas instalações da OTAN, no Quartel de Retamares em Pozuelo de Alarcón, Madrid (figura 9), onde operam atualmente as Unidades mais estratégicas das FFAA espanholas (ECD, 2018).

Figura 9 - Vista aérea da base de Retamares

Fonte: (ECD, 2018)

Hoje em dia, Retamares converteu-se num centro nevrálgico onde se situam algumas das unidades de maior importância estratégica para as FFAA espanholas. Este complexo militar, apelidado de "Pentágono" espanhol, alberga o *Mando de Operaciones* (MOPS), o *Centro de Inteligencia de las Fuerzas Armadas* (CIFAS), o *Mando de Operaciones Especiales* (MCOE) e o MCCD. Já este ano, foi dada luz verde para a construção de um novo edifício para o MCCD, no valor de 10 milhões de euros (ECD, 2018).

3.2.8. Interoperabilidade

O MCCD depende do Chefe do Estado-maior da Defesa, tendo por missão responder às ameaças do ciberespaço ou agressões que possam afetar a Defesa Nacional e cooperar com os centros nacionais de resposta a incidentes de segurança da informação (Onemagazine, 2014).

Há outros organismos na administração espanhola que têm responsabilidades na Cibersegurança: o Centro Criptológico Nacional, pelas administrações públicas; o Ministério do Interior, pelo cibercrime e proteção de IC; e o Ministério da Energia, Turismo e Agenda Digital que está encarregue do Instituto Nacional de Cibersegurança (INCIBE). A coordenação entre todos, deriva da Estratégia Nacional de Cibersegurança, onde também se encontram os organismos do Ministério da Educação e do Fomento (Arce, 2017)

3.3. Síntese conclusiva

Em resposta à QD 2, conclui-se que o modelo de GRH dos militares afetos à estrutura do MCCD é em tudo idêntico ao das restantes FFAA espanholas (Apêndice D). Como CC, em que o pessoal dos três ramos trabalha conjuntamente às ordens do Chefe do

Estado-Maior da Defesa, depende dos RH dos ramos para preenchimento das suas vagas, sem garantia de permanência na função, uma fórmula, similar à utilizada no CCD, dependente da necessidade de rotatividade dos mesmos.

No entanto, podemos aferir algumas diferenças que se destacam pela positiva. Designadamente, uma organização estruturada num CC, planeada com um número significativo de colaboradores militares e civis, cerca de 70, dos quais 49 são militares e 21 são civis, estimando-se que este número possa chegar a 700 nas FFAA, permitindo a sobreposição de funções quando há necessidade de rotatividade. O recrutamento é feito e dirigido a todos os elementos das FFAA, para todas as categorias, o que na prática representa um maior universo de recrutamento que resulta num efetivo aumento do número de militares ligados à CD e SI. A captação de civis passa por atrair indivíduos mais jovens com grande potencial, aos quais se oferece, para além de formação, a oportunidade de trabalhar com tecnologia, procedimentos e outros projetos de infraestruturas aliciantes.

O plano de edificação da capacidade, contempla um plano de formação específica da CD, com formações distribuídas pelos três ramos das FFAA, nas academias e cursos de qualificação, com vista à criação de uma especialidade fundamental de CD. Para além disso, participa em exercícios operacionais de outras Unidades, o que pressupõe um conceito de operações, doutrina própria para as operações no ciberespaço, ou seja, a introdução do ciberespaço em todas as atividades de coordenação e planeamento conjunto, como uma componente integrada.

Desde a criação do MCCD que o seu Comandante-chefe é o General López de Medina, quase a contabilizar 5 anos em funções, que contribui em grande medida para garantir uma edificação estável desta capacidade, bem como o desenvolvimento de planos, como o que decorre neste momento, o plano de consciencialização das FFAA para a CD, sendo considerado essencial para melhorar a cultura cibernética. Também apoia a criação de uma Ciber reserva de *hackers.*

4. Apresentação e análise de resultados

> *Na minha opinião faria muito mais sentido, em termos de pragmatismo, encararmos isto na lógica da especialização.*
>
> Viegas Nunes (2018)

Neste capítulo apresentaremos os resultados das entrevistas efetuadas ao conjunto de entrevistados constantes no Quadro 1. Na sequência dos capítulos anteriores, pretendemos refinar as respostas às QD abordadas nos capítulos anteriores e responder à QD3, bem como apresentar o conjunto de propostas que contribuam para mitigar os problemas apresentados nos capítulos anteriores, que nos ajudarão a atingir o objetivo a que nos propomos e a elaborar as conclusões ao nosso trabalho.

Quadro 1 - Painel de entrevistados

IDENTIFICAÇÃO		FUNÇÃO	DATA
E1	Comodoro Fernando Pires	Diretor da DIRCSI/EMGFA	05ABR18
E2	Cor Tm Viegas Nunes	Cmdt da ECSI da NATO	15MAR18
E3	Cor Tm Camelo dos Santos	Chefe de Gabinete do Cmdt do Pessoal do Exército	05ABR18
E4	CMG Fialho de Jesus	Chefe do CCD	12JAN18
E5	Comodoro Soares Ribeiro	Diretor de Pessoal Marinha	14MAR18
E6	Comodoro Bento Domingues	Superintendente das TI Marinha	05ABR18
E7	Cor Tm Marques da Silva	Cmdt Centro de Trams do Exército	27MAR18
E8	TCor Tm Jorge Vinagreiro	Chefe da Rep. de Guerra da Informação	27MAR18
E9	Cor Luís Graça	Subdiretor da DirPess FA	05MAR18
E10	BGen Passos Morgado	Diretor da DCSI da FA	09ABR18

Fonte: (Autor, 2018)

Os entrevistados, que constituem o painel, foram escolhidos de forma a incluir o leque mais abrangente possível de peritos com vasta experiência nesta área, que tenham desempenhado ou que desempenhem funções nas estruturas dedicadas à CD e SI das FFAA, o que permitiu recolher diferentes visões, que correspondem aos níveis estratégico, operacional e tático. Para atingir este desiderato, recolhemos o contributo de personalidades que desempenham funções fora destas estruturas, no EMGFA e nos três ramos. Ao nível do EMGFA, para além do Chefe do CCD, inquirimos o Diretor da DIRCSI e, ao nível dos ramos, os Diretores das respetivas Direção de Comunicações e Sistemas de Informação (DCSI).

Como o nosso estudo procura melhorar a GRH Ciber, recolhemos também o contributo dos Comandantes ou Diretores do Pessoal dos respetivos ramos, uma vez que são os ramos que alimentam o CCD, em termos de RH, e fazem a sua gestão.

Tendo em conta todo o enquadramento legal e doutrinário da SI e da CD, verificamos que cerca de 90% dos entrevistados considera que os RH afetos a estas atividades nas FFAA, não são suficientes para garantir um nível operacional satisfatório (tabela 2). Para agravar esta escassez de RH, verifica-se um forte assédio de empresas civis sobre os RH das FFAA melhor preparados, o que leva a que metade dos entrevistados considere preocupante a saída nestas condições de militares das FFAA. Esta situação representa uma vulnerabilidade associada, por um lado, ao desapontamento dos militares em questão com a instituição militar e, por outro, às avultadas remunerações que estas empresas civis oferecem.

Tabela 2 - Número de recursos humanos

Segmento resposta	Entrevistados										%
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	
A.1.1- Os RH são suficientes											0
A.1.2- Os RH não são suficientes	X	X	X	X		X	X	X	X	X	90
A.1.3- Saída de militares do QP		X	X				X	X	X		50
A.1.4- Não compete responder					X						10

Fonte: (Autor, 2018)

Numa segunda questão, foi perguntado aos entrevistados que medidas poderiam ser implementadas para melhorar a gestão destes RH e 90% referiu a necessidade de ajustamento dos QO afetos às estruturas de SI e CD das FFAA (tabela 3). Se associarmos esta percentagem com a da questão anterior, podemos inferir que ambas estão relacionadas, pois se, na anterior, 90% dos inquiridos refere que os RH são insuficientes, naturalmente e na mesma lógica para colmatar esta insuficiência os QO terão de ser alargados.

Há situações em que, para além do QO não ser o mais ajustado, o quadro de efetivos não corresponde ao QO, como é o caso do CCD e do CIRC do Exército. No caso do Exército, esta situação ainda é mais grave porque, dos sete militares que compõem este CIRC, existem apenas três oficiais e nenhum dos 3 sargentos previstos.

Por outro lado, cerca de 70% dos inquiridos elegem a formação dos RH como uma melhoria a efetuar. Também, aqui, podemos relacionar esta elevada percentagem a outra melhoria considerada por 70% dos peritos, que é o retorno do investimento na formação com maior tempo de inamovibilidade na função. Apesar dos militares selecionados para desempenho de funções nas estruturas dedicadas à CD e SI possuírem algum tipo de formação base, esta necessita de ser complementada com formação específica,

normalmente demorada e onerosa. Portanto, considera-se elementar retirar o máximo proveito deste investimento em formação, o que muitas das vezes não acontece. Adicionalmente, a formação deverá estar associada à prática e à experiência que só se adquirem em contato diário e prolongado com esta realidade. Ora, como referem 70% dos inquiridos, é necessário formar, garantir experiência e garantir um período de tempo adequado, cerca de oito anos, para se retirar o proveito máximo desse investimento.

Tabela 3 – Implementação de melhorias de GRH

Segmento resposta	Entrevistados										%
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	
A.2.1- Uma GRH diferenciada								X			10
A.2.2- Retorno da formação e inamovibilidade na função	X	X			X	X		X	X	X	70
A.2.3- Equivalência às condições de promoção								X			10
A.2.4- Percurso profissional								X			10
A.2.5- QO adequado	X		X	X	X	X	X	X	X	X	90
A.2.6- Formação dos RH	X	X		X	X	X	X			X	70

Fonte: (Autor, 2018)

No que respeita à criação de um novo QEC nas FFAA, 90% dos entrevistados consideram que na conjuntura atual não faz sentido (tabela 4). Por um lado, a dimensão das nossas FFAA não justificam a sua criação e, por outro, a sua implementação acarretaria implicações a vários níveis, nomeadamente ao nível da formação nas academias, de forma a garantir a sua alimentação, bem como a sua operacionalização entre Marinha, Exército e FA.

Depois, o número de militares afetos às estruturas de CD e SI, ainda que a curto prazo venham a ser aumentados os QO, é diminuto e, como não garante grandes perspetivas de carreira, torna-se pouco atrativa. Apesar de atualmente este QEC não fazer sentido, atendendo que esta capacidade está permanentemente em crescimento, a longo prazo poderá vir a ser uma realidade, obviamente com todas as vantagens que daí decorrem para a GRH.

Embora não tenha sido perguntado, cerca de 60 % dos inquiridos referiram que a criação de uma especialização na área Ciber, com base numa formação, faz todo o sentido, sobretudo, se esta for uniformizada nas FFAA, garantindo-se, assim, uma formação base igual para todos os militares e o aumento da base de seleção dentro das FFAA.

Para esta especialização, poderiam ser potencializadas sinergias existentes nos ramos, como é o caso do Regimento de Transmissões do Exército do Porto, capaz de garantir esta especialização e que passaria a ser um denominador comum nesta área. Naturalmente que esta especialização seria prioritariamente garantida aos militares que

apresentassem maior potencial e apetência para as funções, de forma a desenvolverem as suas capacidades nesta área.

Tabela 4 - Criação de um QE Ciber

Segmento resposta	Entrevistado										%
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	
A.3.1- Faz sentido											0
A.3.2- Não faz sentido	X	X	X		X	X	X	X	X	X	90
A.3.3- Não responde				X							10
A.3.4- Uma especialidade		X	X		X	X	X		X		60

Fonte: (Autor, 2018)

No que respeita à contratação de especialistas civis, os entrevistados assumem, claramente, ter vantagens. Uma dessas vantagens - segmento que recolheu cerca de 80% das respostas (tabela 5), é que, como esta área não se compadece com a rotação a curto prazo dos elementos que nela trabalham, pode garantir maior permanência na função, maior estabilidade de colocação. Outra vantagem, que reuniu 70% das respostas, prende-se com a colmatação da falta de militares, dado que estes estão sujeitos a períodos de inamovibilidade curtos.

De salientar, igualmente, que 60% dos inquiridos refere que a contratação de civis é de difícil concretização por várias ordens de razão. A procura de especialistas aumentou e as entidades privadas conseguem oferecer melhores condições contratuais, nomeadamente, níveis remuneratórios muito mais elevados. Embora estes civis possam ser contratados numa fase precoce da sua atividade laboral, à medida que forem angariando formação e adquirindo experiência, será cada vez mais difícil, devido ao assédio das empresas civis, segurá-los na instituição militar. Outros referem, ainda, a necessidade de uma gestão de civis, pelo que propõem a contratação de empresas para a prestação destes serviços com requisitos de S*ervice Level Agreements* adequados às necessidades militares.

Tabela 5 - Contratação de especialistas civis

Segmento resposta	Entrevistado										%
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	
A.4.1- Maior permanência na função	X		X	X		X	X	X	X	X	80
A.4.2- Mitigação da falta de militares	X	X			X	X	X	X		X	70
A.4.3- Maior especialização técnica	X	X						X			30
A.4.4- Limitação de emprego em op. militares	X							X		X	30
A.4.5- Difícil concretização	X		X			X	X	X	X		60
A.4.6- Não contratação					X						10

Fonte: (Autor, 2018)

Curioso que, apesar de três dos entrevistados referirem como desvantagem o emprego de civis em operações militares, como uma limitação, em sentido contrário, um deles refere que só se conseguirá implementar eficazmente a capacidade de CD com emprego de civis, obviamente inseridos em equipas, devidamente enquadradas por militares que definam as ações a desenvolver.

Na quinta e última questão, que foi à procura das medidas a serem adotadas para melhorar a retenção destes elementos na função, constata-se uma maior dispersão das respostas, pelo que a tabela apenas reflete as que tiveram maior expressão (tabela 6). Desta forma, para além de uma análise tendo em conta a expressão quantitativa de resposta aos segmentos, esta questão será complementada com outros contributos diferenciados.

Cerca de 60% dos inquiridos responderam que deve ser aumentado o período de inamovibilidade na função. Efetivamente, os estudos indicam que só ao fim de cinco é que um analista forense está preparado para lidar com todas as situações com que se pode deparar no âmbito da CS e da CD. Paralelamente, se associarmos este período à formação especializada exigida, ao treino e à prática, o período de inamovibilidade mais ajustado seria de oito anos. No entanto, oito anos, relativamente à carreira militar, é um período muito longo que poderá colidir com alguns processos e pressupostos legais exigidos aos militares.

No que respeita à valorização da carreira, cerca de 50% dos inquiridos propõem melhorias para que se torne atrativa, singular, tanto porque permite desenvolver atividades que noutro enquadramento poderiam ser consideradas ilegais, ou por ser uma área de ponta, relevante e importante para o país e ao mesmo tempo compensadora. Ao nível das recompensas, apenas 30% dos entrevistados refere a melhoria remuneratória como um fator determinante para aumentar a retenção das pessoas nestas funções. No entanto, verificamos que os militares que abandonam a instituição militar e desenvolvem a sua atividade profissional no mundo civil auferem vencimentos 400% superior aos que auferiam nas FFAA.

O desenvolvimento profissional, respondido por 40% dos entrevistados, está diretamente relacionado com as caraterísticas dos RH tipicamente afetos a esta realidade, uma vez que demonstram gosto e interesse por estas temáticas, pela sua aprendizagem, associada à necessidade constante de atualização para acompanharem a permanente evolução tecnológica. O desenvolvimento profissional também tem de ser considerado para atrair RH civis, pois, como os especialistas mais experientes são inacessíveis, a alternativa será contratar jovens com a formação básica efetuada e garantir-lhes pacotes de

especialização a troco de um período de permanência, a considerar, mas nunca inferior a oito anos, que lhes permita um desenvolvimento de carreira diferenciado e lhes garanta o acesso ao mercado de trabalho sem grandes problemas.

Como referido aquando da análise efetuada às respostas da tabela seis, cerca de 60% dos inquiridos referiram a necessidade de uma especialização comum na área Ciber às FFAA. A esta questão, cerca de 40% dos entrevistados, elencaram, como medida de melhoria da retenção, a formação base igual nos três ramos. Se considerarmos a formação base, podemos aferir que cerca de 80% dos inquiridos, pela conjugação das duas respostas, referem a necessidade de criação de uma formação base comum nos três ramos, ou seja, uma especialização comum. Algumas vantagens seriam evidentes. Logo à partida, uma das vantagens da formação comum para colmatar a falta de RH afetos a esta atividade, evidenciada por cerca de 90% dos inquiridos, é a possibilidade de aumentar o universo de recrutamento a todos os elementos das FFAA e a possibilidade de selecionar praças, sargentos e oficiais para desempenho de funções diferenciadas, de acordo com a sua especialização e posto. Por outro lado, seria um denominador comum que aumentaria o sentimento de uniformidade nas FFAA perante as questões relacionadas com a CD e a SI e favoreceria uma maior consciencialização institucional. Considerar-se-ia, adicionalmente, caso houvesse essa intenção, a atribuição de um suplemento remuneratório, tendo por base esta especialização e o desempenho de funções na área.

É, também, de referir a necessidade de uma GRH Ciber criteriosa ou diferenciada que, apesar de mencionada diretamente apenas por dois entrevistados, é transversal a todas as respostas referentes a esta questão e anteriores, uma vez que a GRH compreende um conjunto de atividades concorrentes para o mesmo fim. Embora o nosso estudo tenha incidido nos aspetos referentes à seleção e recrutamento, formação e treino e retenção, todos dizem respeito à GRH.

Outro aspeto importante que sobressai do conteúdo das entrevistas é a necessidade de tornar a GRH mais flexível e adaptada a estes RH, deixando de ser mais um entrave à gestão eficaz destes recursos especializados. Esta gestão terá sempre de ter como princípio orientador a garantia das mesmas condições de desenvolvimento da carreira e iguais oportunidades de progressão de carreira. No entanto, verifica-se que se tem constituído como um obstáculo, relativamente às transferências e colocações, cursos de formação e requisitos de promoção. Nada é mais desmotivante para um recurso altamente especializado, tecnicamente capaz e valorizado e que satisfaz profissionalmente, do que ser deslocado e ir desempenhar funções ordinárias que poderiam ser exercidas por outros. A

este facto acresce a inexistência de alternativas oferecidas pela instituição, não há uma carreira técnica horizontal e se abdicar da promoção é prejudicado financeiramente. Portanto, é necessário que as FFAA olhem para aquilo que está ao seu alcance e, tanto quanto possível, implementem medidas de caráter excecionais, incrementado o bem-estar destes RH, indo ao encontro das suas aspirações e dos interesses da instituição.

Outros contributos, embora menos expressivos em termos de quantidade mas que pela sua pertinência são de considerar, seria a constituição de uma reserva cibernética de pessoal, com experiência no desempenhado de funções nas FFAA e que, sob determinadas condições a serem determinadas, estaria disponível para apoiar em casos de necessidade. Esta situação poderia ser mais um incentivo à prestação do serviço militar, permitindo que os militares, após terminarem o seu contrato de longa duração, sob determinadas condições, permanecessem neste tipo de estruturas na condição de reservista.

Outras medidas, mais relacionadas com a cultura Ciber e a valorização da carreira, seriam a adoção de medidas para aumentar o bem-estar e satisfação profissional dos militares, tais como: a formação avançada de qualidade sobre tecnologia de ponta; a valorização do trabalho desenvolvido de forma a criar um sentimento de utilidade nacional; e a garantia de continuidade temporal em funções relacionadas com o percurso formativo e de especialização.

Tabela 6 - Medidas de melhoria da retenção

Segmento resposta	Entrevistado										%
	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	
A.5.1- Gestão criteriosa					X			X			20
A.5.2- Formação base igual nos 3 ramos	X	X	X	X							40
A.5.3-Melhoria remuneratória		X					X		X		30
A.5.4- Aumento do período de inamovibilidade	X	X			X		X	X		X	60
A.5.5- Desenvolvimento profissional	X	X				X	X				40
A.5.6- Valorização da carreira Ciber		X	X			X	X		X		50

Fonte (Autor, 2018)

Conclusões

> "*Cyber is the number-one threat to national security, and people, not technology, will out think and out maneuver these cyber threats*."
>
> General Rhett Hernandez (Stewart, 2013)

Para melhor reflexão e análise, importa relembrar as grandes linhas do procedimento metodológico seguido na nossa investigação, à qual presidiu o seu OG, designadamente o apuramento do modelo de GRH que melhor se adequa aos militares especializados em CD e SI das FFAA, de forma a obter ganhos operacionais nesta capacidade, e que nos levou à construção da nossa QC: Como poderá ser otimizada a GRH Ciber nas estruturas Ciber das FFAA? Delineámos três QD que concorreram para dar resposta à nossa QC e que, de forma sequencial, foram sendo respondidas ao longo dos capítulos segundo, terceiro e quarto, pelo desenvolvimento de uma estratégia de investigação qualitativa, recorrendo essencialmente ao raciocínio do tipo indutivo.

Desta forma, depois de avaliar a capacidade de CD face à GRH, dos elementos que trabalham no CCD, relativamente aos fatores relacionados com a seleção, formação e treino e a retenção, procedemos a esta avaliação na estrutura equivalente em Espanha, de forma sistematizada, garantindo a necessária facilidade de comparação e análise crítica, e dando corpo ao desenho de pesquisa adotado, do tipo comparativo. Aqui, importa referir que Portugal, ao contrário dos outros países da OTAN, possui um centro de CD, mas que, tendo em conta as últimas declarações do MDN, a Diretiva Estratégica do CEMGFA e militares peritos, a curto prazo espera-se a evolução do CCD a CC. Por outro lado, a escolha do MCCD mostrou ser a melhor opção em termos de acesso de informação, que embora se apresente desigual relativamente à dimensão das respetivas FFAA, em nada desvirtua a sua escolha, numa lógica assente na procura de melhores processos e metodologias de GRH.

Perante a caraterização destes dois processos de GRH, o português e o espanhol, procurou-se, através da realização de entrevistas semiestruturadas a peritos no âmbito da CD e SI e a responsáveis pelos órgãos de gestão de pessoal dos três ramos das FFAA, não só, complementar esta informação, como, também, recolher os seus contributos para mitigar as vulnerabilidades encontradas e potenciar os aspetos que podem ser aperfeiçoados, com vista aumentar a capacidade de CD.

No primeiro capítulo, apresentámos, de forma sistematizada, o enquadramento concetual necessário para o desenvolvimento da nossa investigação, bem como delineámos, de forma aprofundada, o percurso metodológico necessário para a sua concretização.

No segundo capítulo, respondemos à QD1, analisando o atual impacto que a GRH tem na capacidade de CD, com recurso à metodologia DOTMLPI-I, utilizada na edificação de capacidades operacionais. Demos especial relevância à Organização, Treino, Liderança e Pessoal, pois estes são influenciados diretamente pelos RH, que constituem o centro de gravidade da capacidade de CD, capazes de defender e se necessário atacar as fontes das ameaças Ciber. Só com um efetivo adequado de RH é possível constituir equipas e treinar procedimentos, garantindo assim uma resposta à altura das ameaças. O reduzido número de elementos, e a incontornável rotatividade desses elementos, consequência da comissão de serviço e da manutenção dos direitos e das garantias de progressão de carreira, definem a GRH Ciber, em nada diferente das FFAA em geral, e compromete esta capacidade. Daqui resulta que o principal desafio às FFAA é recrutar e reter o pessoal mais qualificado, promovendo o seu treino, conhecimento e competências técnicas.

No terceiro capítulo, recorrendo uma vez mais à metodologia DOTMLPI-I da OTAN, analisámos a capacidade de CD do MCCD, o que nos permitiu apurar qual o modelo de GRH aqui empregue, respondendo assim à QD2. Concluiu-se que o modelo de GRH dos militares afetos à estrutura do MCCD é idêntico às restantes FFAA espanholas, que recorre aos RH dos ramos, sem garantia de permanência na função, e que está dependente da necessidade de rotatividade dos mesmos. Está organizado segundo um CC, com cerca de 70 elementos, dos quais 49 são militares e 21 e são civis. O recrutamento militar, que tem como universo as FFAA, abrange todas as categorias, uma fórmula mais abrangente que a utilizada no CCD, o que resulta no aumento efetivo de militares afetos à CD e SI. Por outro lado, a captação de civis passa por atrair indivíduos, mais jovens, com grande potencial, aos quais se oferece a oportunidade de trabalhar com tecnologia, procedimentos e outros projetos aliciantes.

De sublinhar a importância do seu plano de edificação da capacidade, que contempla uma formação específica de CD, com formações distribuídas pelos três ramos das FFAA, nas academias e cursos de qualificação, que, em última análise, permitem a criação de uma especialização fundamental de CD. Compreendendo a importância de uma liderança forte e duradoura, o comandante do MCCD está em funções há quase cinco anos, garantindo estabilidade na prossecução das medidas de implementação e no desenvolvimento de

planos de consciencialização das FFAA para a CD, com vista a melhorar a cultura cibernética.

No quarto capítulo, procurámos complementar os dois capítulos anteriores, aprofundando as dificuldades sentidas no impacto da GRH na capacidade de CD nacional e, ao mesmo tempo, procurando contributos para a melhoria dessa mesma gestão de pessoal, concretizados em medidas a implementar, respondendo assim à QD3. À partida, concluímos unanimemente que os RH afetos à CD e SI são insuficientes para garantir um nível operacional satisfatório e que as FFAA têm de lidar com o forte assédio exercido por empresas civis que procuram para os seus quadros especialistas nesta área. Uma vez que os RH são insuficientes, surge a necessidade de aumento dos QO afetos às estruturas dedicadas, sendo necessário, para os completar, aumentar o universo de recrutamento à totalidade das FFAA, a todas as categorias, complementado com um plano de formação base e específico para os candidatos a ciberguerreiros. Esta formação fundamental seria a base para a criação de uma especialização Ciber no âmbito das FFAA.

Quanto à criação QEC na conjuntura atual, não faz sentido, porque o número de militares afetos às estruturas de CD e SI é diminuto e não possibilita um percurso nem perspetivas de carreira.

Foram evidentes as vantagens da contratação de especialistas civis, pois, a garantia de permanência e estabilidade na função, permitirão colmatar a falta de militares. A concretização desta solução passará pela contratação destes, numa fase precoce da sua atividade laboral, garantindo-lhes formação e experiência a troco de um período de permanência, que no final constituirá uma mais-valia e permitirá que sejam rapidamente absorvidos pelo mercado de trabalho. Os baixos níveis remuneratórios oferecidos são uma dificuldade à contratação de civis mas a sua gestão pode ser ultrapassada contratando empresas com S*ervice Level Agreements* adequados às necessidades militares.

As medidas para melhoria da retenção passam por aumentar o período de inamovibilidade na função para os oito anos, pela valorização da carreira profissional, tornando-a mais atrativa, pela compensação do nível remuneratória, através de um suplemento funcional com base numa formação de acesso a uma especialidade, por fomentar o desenvolvimento profissional, indo ao encontro das expectativas destes RH, e por permitir a atualização de conhecimento a par com a evolução tecnológica. A implementação de uma GRH Ciber diferenciada, mais flexível e adaptada a estes RH, deve ser seguida, através da implementação de medidas de caráter excecional, indo ao encontro

das aspirações dos militares e dos interesses da instituição, garantindo sempre as mesmas condições de desenvolvimento da carreira e iguais oportunidades de progressão de carreira.

Perante este percurso, iniciado com a análise do impacto da atual GRH na capacidade de CD do CCD, seguido da compreensão do modelo de GRH utilizado no MCCD e, finalmente, pela recolha de contributos dos peritos na área Ciber e dos responsáveis pela gestão dos RH das FFAA, consideramos estar em condições de responder à nossa QC, como é que a GRH Ciber poderá ser otimizada, pelo que propomos o nosso modelo de GRH Ciber. Para melhor compreensão vamos sistematizar as medidas a adotar ao modelo de GRH Ciber, partindo da seleção e recrutamento, passando pela formação e treino e terminando na retenção.

Relativamente à seleção e recrutamento, esta deve assentar num modelo misto, ou seja, recrutar, internamente, dentro das FFAA e, exteriormente, recorrendo a pessoal civil. Este rácio, entre militares e civis, deve ser equilibrado, de acordo com as necessidades, sendo que no MCCD é na ordem dos 25%, portanto, um quarto do QO. Os militares a selecionar devem abranger todo o espectro das FFAA, dirigido a oficiais, sargentos e praças, de acordo com os diversos papéis a desempenhar. A aposta nos civis deve ser feita em técnicos formados recentemente, com pouca experiência mas com potencial de desenvolvimento. Uma forma de os atrair às FFAA será garantir formação, especialização, oportunidade de desenvolvimento e acumulação de experiência, que, certamente, os valorizará e lhes garantirá boas oportunidades no mercado de trabalho após términus do compromisso contratual. Estes efetivos, podem ser complementados com a constituição de uma reserva *hacker,* formada, por exemplo, por reservistas das FFAA.

No que à formação diz respeito, vamos tecer considerandos relativos à formação em si, treino, experiência e especialização. Ficou bem patente, nos capítulos precedentes, a necessidade de aumento do número de militares afetos a esta atividade, pelo que se torna fundamental garantir as competências necessárias ao desempenho das funções destes novos elementos. Daí que, à cabeça da formação, deve de ser idealizado e implementado um plano de formação, capaz de responder às exigentes necessidades de alimentar as estruturas dedicadas às CD e SI. Este plano deve ser estruturado para garantir diferentes tipos especialização, de acordo com as funções a desempenhar, e deve abranger as academias militares das FFAA e, também, ter em conta as estruturas de formação já existentes nesta área, potencializando-as, como é o caso do Regimento de Transmissões do Exército no Porto. Este plano permitirá o aumento do universo de recrutamento, a alimentação das

estruturas com RH especializados, a uniformização da formação Ciber nas FFAA, a maior consciencialização Ciber no seio das FFAA e o fomento da cultura Ciber.

Quanto ao treino, é fundamental a continuação da participação das equipas nacionais nos melhores exercícios realizados ao nível internacional e nacional, essenciais para treinar e perceber lacunas na formação. De louvar, a adesão de Portugal ao CCDCOE da OTAN e o MN CD E&T, que têm de ser explorados ao máximo em proveito dos nossos RH. Existe uma lacuna relativamente à execução de exercícios operacionais que, com a passagem do CCD a um CC, progressivamente tem de ser colmatada, passando o planeamento e execução de exercícios a serem realizados como uma componente integrada. O *know how*, acumulado pelos militares, resultante da experiência e do tempo de permanência em funções, deve ser preservado e transmitido para que o mesmo não se perca com a saída destes elementos.

Não menos importante será a necessária criação e implementação de uma especialização Ciber comum às FFAA. Esta especialização teria como base um curso de formação, orientada e de acordo com as necessidades das FFAA, e, portanto, teria de estar inserida no plano de formação, concorrendo em paralelo para os seus objetivos, permitindo, ainda, a criação e a base de um suplemento remuneratório, a atribuir a estes especialistas que desempenhassem funções na área.

Uma vez que a criação do QEC, na conjuntura atual, como referido, não faz sentido, passemos agora à questão da retenção, acerca da qual abordaremos os aspetos relativos à sua gestão diferenciada, ao desenvolvimento pessoal, carreira, tempo de permanência na função e remuneração. Quanto à GRH destes elementos Ciber, tem de se promover, com o incremento da cultura organizacional Ciber, para a qual concorrem diversos fatores, uma maior consciencialização dos decisores, nomeadamente, dos órgãos de gestão de pessoal, pois é necessária uma gestão diferenciada destes recursos, uma vez que são escassos e foram sujeitos a uma formação com elevado nível investimento, quer em patrocínio quer em termos temporais.

Outro ponto, prende-se com a conciliação entre os interesses institucionais e os interesses pessoais, à luz dos princípios consignados legalmente no EMFAR e lei fundamental.

Internamente, ao nível dos órgãos de gestão de pessoal das FFAA, terá de haver uma consciencialização que possibilite a flexibilização dos aspetos relativos à gestão destes elementos, que permita a adaptação dos requisitos relacionados com a promoção, nomeadamente cursos de promoção, tempo de comando e outros, podendo, nestes aspetos,

a instituição militar adaptar-se e escrutinar exceções razoáveis e atendíveis à gestão destes RH.

Quanto ao desenvolvimento pessoal, este aspeto está relacionado com as caraterísticas destes profissionais, as suas necessidades e as suas expectativas. Quem se dedica a esta área, tem necessidade de se atualizar para se manter a par com as evoluções tecnológicas, tem gosto e apetência natural por aprender, pelo que, permitir ou garantir a aprendizagem a estes elementos em áreas da vanguarda do desenvolvimento, potenciando depois esta aprendizagem diferenciada em projetos aliciantes e inovadores, constitui um fator que ajuda à sua retenção. Esta estratégia permitirá, ainda, criar um sentimento de utilidade pública, pelo contributo gerado para o bem-estar da sociedade. No entanto, este aspeto encerra uma desvantagem que se prende com o proporcional aumento do assédio sobre estes militares, por parte de empresas civis.

No que à carreira diz respeito, há a referir duas modalidades essenciais. Primeiro, para aqueles que optem por uma carreira vertical, com ascensão nos postos, refira-se um aspeto positivo, que já está implementado mas que pode ser melhorado, que é fazer uma gestão em termos de transferências e colocações destes militares, entre as estruturas dos ramos e do EMGFA, tirando, assim, partido desta possibilidade e do jogo entre promoções e atribuição de funções. Desta forma, possibilita-se ascensão na carreira e ao mesmo tempo a manutenção destes recursos em funções relacionadas com esta área. Outra forma de aumentar a retenção dos militares é permitir a opção por uma carreira diferente da vertical. Este mecanismo já está previsto no EMFAR, no entanto, ainda não está regulado e muito menos implementado nas FFAA. Em determinadas funções, como é o caso das relacionadas com a área Ciber, esta opção permitiria segurar recursos válidos, motivados pelo seu trabalho, sem que fossem prejudicados em termos remuneratórios, de regalias e condições de reforma.

Quanto ao tempo de inamovibilidade, é de referir que a possibilidade de permanecer cinco anos nas estruturas do EMGFA, apesar de permitir alguma permanência, pode ser aumentada e devidamente prevista e enquadrada. Designadamente, é necessário proceder a uma uniformização legal, quanto ao tempo de permanência no CCD, porque entre as OPC, a LO do EMGFA e os normativos dos ramos, não existe uniformização, sendo, efetivamente, necessária uma determinação legal que preveja o tempo de permanência no CCD ou no futuro CC. Tendo em linha de conta o tempo despendido em formação e especialização e o necessário à maturação destas habilidades, consideramos necessário aumentar o tempo de permanência, sem descurar os princípios de GRH e as garantias de

igualdade oportunidade de carreira. Este período temporal seria, então, de oito anos para os militares e, para os elementos civis, nunca inferior a esses oito. O tempo de permanência dos Comandantes ou Chefes deveria, também, acompanhar este aumento e nunca inferior a cinco anos para garantir o desenvolvimento da sua estratégia.

O último aspeto, referente à retenção, prende-se com a melhoria do índice remuneratório. Um fator que pode ajudar à retenção dos militares será a atribuição de um suplemento remuneratório de especialidade, com base na formação específica e no desempenho de funções nas estruturas Ciber.

Com estas medidas, designadamente ao nível da seleção e recrutamento, formação e treino e retenção, enquadradas num modelo de GRH Ciber que abranja todos os aspetos a ele relacionados, pretende-se obter ganhos e melhorar a capacidade operacional das estruturas Ciber das FFAA.

No nosso caso, a resposta à QC vai ao encontro das recomendações, uma vez que estas estão contidas nesta resposta. Relembrando as que consideramos mais importantes, sublinhamos a implementação de um plano de formação, essencial, como vimos, para melhoria de vários aspetos, indo ao encontro da real constatação de que as pessoas e o seu conhecimento são o cerne da verdadeira capacidade. Em consequência da implementação deste, a criação de uma especialização alicerçado no curso de formação e, por último, a disponibilização de opções válidas, que constituam verdadeiramente uma alternativa que vá de encontro aos interesses da instituição e das expectativas dos militares, nomeadamente, a regulamentação e implementação das carreiras técnicas ou horizontais.

No que diz respeito às limitações da investigação, elas prenderam-se, essencialmente, com a falta de informação disponível referente à GRH Ciber, ou seja, como é que esta gestão é efetuada e em que aspetos se diferencia da geral. Esta falta de informação deve-se, sobretudo, à classificação destes elementos como reservados ou mesmo confidenciais, facto perfeitamente compreensível mas que dificultou a nossa investigação. Outros aspetos que dificultaram a recolha de informação, foi a quase inexistente literatura relacionada com os RH Ciber e a sua gestão, provavelmente porque esta problemática é muito recente, são estruturas muito recentes, como, por exemplo, a criação de um sexto ramo Ciber nas FFAA alemãs que tem de cimentar para que se percebam as suas vantagens. A constante maturação desta realidade faz com que haja uma evolução permanente nas mesmas, situação a que Portugal também não é alheio, como disso é demonstrativo a orientação política para o ciclo de Planeamento de Defesa Militar e a Diretiva Estratégica do EMGFA 2018/2021, que, a curto prazo, vão trazer alterações à realidade atual.

Se a nível nacional esta dificuldade esteve presente, mais difícil ainda foi obter informação acerca da GRH das estruturas estrangeiras, nomeadamente a relativa ao MCCD, que, só após várias insistências, respondeu à solicitação e de forma muito contida, tendo sido, portanto, necessário recorrer aos préstimos dos Major Juan Rodriguez, Engenheiro do Exército espanhol e auditor do CEMC 2017/2018, para alguns esclarecimentos adicionais.

No que concerne a pesquisas futuras e como consideramos essencial a sua implementação, deverá ser efetuado um estudo acerca da implementação do plano de formação Ciber para as FFAA. Este estudo deverá ir além dos pressupostos necessários à sua implementação e perceber o seu impacto ao nível das estruturas de ensino militares.

Seria oportuna a criação de protocolos entre as FFAA e os centros universitários, com vista à captação de jovens talentos recém formados, facilitando a sua contratação. A regulamentação da carreira horizontal, prevista no EMFAR, deverá avançar de forma a constituir-se como uma opção válida e de escolha alternativa à realidade atual. Dado que os recursos económicos são escassos, é pertinente estudar o impacto orçamental respeitante à implementação do plano de formação Ciber, bem como para a criação de um suplemento remuneratório a atribuir aos especialistas Ciber.

Bibliografia

Agência Lusa, 2018. *Portugal junta-se ao grupo de países mais avançados da NATO em `ciberdefesa´* [Em linha] Observador. Disponível em: https://observador.pt/2018/04/23/portugal-junta-se-ao-grupo-de-paises-mais-avancados-da-nato-em-ciberdefesa/, [Acedido em 02 Mai. 2018]

Ágreda, Á., 2016. El Modelo de Ciberseguridad y Ciberdefensa en España In: Pinto J., 2016. *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional*. Rio de Janeiro: ESG.

AJP-3.10, 2009. *Allied Joint Doctrine for Information Operations.* Bruxelas: NATO.

Álvaréz, M., 2017. *«No hay paz en el ciberespacio»* [Em linha] Disponível em: http://www.eldiariomontanes.es/cantabria/ciberespacio-20170926151902-nt.html, [Acedido em 23 Mar. 2018].

Andress e Winterfeld, J. S., 2011. *Cyber Warfare Techniques, Tactics and Tools for Security Practitioners.* Waltham: Elsevier.

Arce, R., 2017. *General Medina: "Todos los días tenemos que defendernos de ciberataques"* [Em linha] The Objective. Disponível em: http://theobjective.com/further/general-medina-todos-los-dias-tenemos-que-defendernos-de-ciberataques/, [Acedido em 23 Mar. 2018].

Assunção, F., 2018. O Conceito de Ciberdefesa: evolução e perspetivas para Portugal.In: IUM 2018. Seminário de operações do CEMC 2017/18: *Ciberdefesa e Cooperação Civil-Militar*. 09 de abril de 2018. Pedrouços.

Belt, 2013. *España invertirá 4,8 millones para impulsar su nuevo Mando de Ciberdefensa* [Em linha] Disponível em: http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=16548, [Acedido em 22 Mar. 2018].

Bryman, A., 2012. *Social Research Methods*. 4ª ed. Oxford: Oxford University Press.

Carneiro, A., 2016. A Defesa Cibernética como Extensão do Papel Constitucional das Forças Armadas na Defesa Nacional In: Pinto J., 2016. *Ciberdefesa e Cibersegurança: Novas Ameaças à Segurança Nacional.* Rio de Janeiro: ESG.

Ceitil, M., 2002. O Papel da Formação no Desenvolvimento de Novas Competências IN: *Gestão dos Recursos Humanos: Contextos, Processos e Técnicas*. 2º ed. Lisboa: Editora RH.

Cendoya, A., 2016. *National Cyber Security Organisation: SPAIN*. [Em linha] NATO Cooperative Cyber Defense Centre of Excellence, Tallinn, Estonia. Disponível em:

https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_SPAIN_092016.pdf, [Acedido em 27 Jan. 2018].

CM, 2013a. *Aprovou o Conceito Estratégico de Defesa Nacional* (RCM n.º 19/2013 de 05 de abril) Lisboa: DR.

CM, 2013b. *Aprovou a reforma estrutural da Defesa Nacional e das Forças Armadas* (RCM n.º 26/2013, de 11 de abril). Lisboa: DR.

CM, 2014. *Aprovou a Lei Orgânica do EMGFA*. (DL n.º184/2014 de 29 de dezembro). lisboa:DR.

CM, 2015a. *Aprovou o Estatuto dos Militares das Forças Armadas* (Decreto-Lei n.º 90/2015 de 29 de maio). Lisboa: DR.

CM, 2015b. *Aprovou a organização interna das unidades, estabelecimentos e órgãos do EMGFA (DR 13/2015 de 31 de julho).* Lisboa: DR.

CM, 2015c. *Aprovou a Estratégia Nacional de Segurança do Ciberespaço* (RCM 36/2015 de 28 de maio). Lisboa: DR.

CM, 2017. *Aprovou a criação do Conselho Superior de Segurança no Ciberespaço* (Resolução do Conselho de Ministros n.º 115/2017 de 24 de agosto) lisboa: DR.

CM, 2018. *Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016* (Comunicado do Conselho de Ministros de 15 de março de 2018) Lisboa: DR.

Conti, G. e Easterly, J., 2010. *Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture* [Em linha] Small Wars Journal, Disponível em: http://smallwarsjournal.com/blog/journal/docs-temp/482-conti-easterly.pdf, [Acedido em 20 Fev. 2018].

Costa, J., 2017. *Cntributos para a definição das Competências do Centro Nacional de Ciberdefesa no Panorama da Cibersegurança Nacional: a Definição de Responsabilidades e a Coordenação com os Diferentes Autores.* TII do CPOSFA 2016/2017. IUM. Lisboa: IUM.

DICSI/EMGFA, 2013. *Plano para a Edificação da Capacidade de Ciberdefesa Nacional.* Lisboa: EMGFA.

Domingues, B., 2018. *A criação de Quadro Especial Ciber.* [Entrevista] Lisboa (05 abril 2018).

Durán, J., 2010. Capítulo V La Ciberseguridad en el Ámbito Militar IN: *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio,* Cuadernos de

Estrategia N.º 149, Ministerio de Defensa. Madrid: Imprenta del Ministerio de Defensa.

ECD, 2018. *El 'Pentágono' español de Retamares va tomando forma* [Em linha] El Confidencial Digital, Disponível em: https://www.elconfidencialdigital.com/defensa/Pentagono-espanol-Retamares-tomando-forma_0_2858714109.html, [Acedido em 22 Mar.2018].

EM da Defensa, 2018. *Mando Conjunto de Ciberdefensa.*[Em linha]Estado Mayor de la Defensa. Disponível em: http://www.emad.mde.es/CIBERDEFENSA/, [Acedido em 14 Fev. 2018].

EM MCCD, 2018. *A Criação de um Quadro Especial Ciber. Entrevista ao Chefe do Centro de Ciberdefesa do EMGFA.* [Entrevista] Lisboa (03 abril 2018).

EMAD, 2018. *Organograma do Estado Mayor de la Defensa [Em linha] Disponível em: http://www.emad.mde.es/EMAD/novemad/multimedia/fotos_EMAD/2014/10/141017-emad-general-final.jpg, [Acedido em 26 Mar. 2018]*.

EMD, 2013. *General de División Carlos Gómez López de Medina* [Em linha] MCCD, Estado Mayor de la Defensa. Disponível em: http://www.emad.mde.es/CIBERDEFENSA/mando/index.html [Acedido em 23 Mar. 2018].

Europapress, 2013. *El mando de Ciberdefensa, listo para empezar a trabajar* [Em linha] Disponível em: http://www.europapress.es/nacional/noticia-mando-ciberdefensa-ya-dispone-sede-medios-tecnicos-empezar-trabajar-siete-meses-despues-creacion-20130930184225.html, [Acedido em 23 Mar. 2018].

Evans, K. e Reeder, F., 2010. *A Human Capital Crisis in Cybersecurity. Technical Proficiency Matters.* Center for Strategic and International Studies. Washington: CSIS.

Fernandes, L., 2002. Evolução do Mercado de Trabalho e Sistemas Salariais IN: *Gestão dos Recursos Humanos: Contextos, Processos e Técnicas.* 2ª ed. Lisboa: Editora RH.

Franz, T., 2011. *The Cyber Warfare Professional. Realizations for Developing the Next Generation [Em linha] Air & Space Power Journal pp 87 - 99. Disponível em: https://www.hsdl.org/?view&did=5454, [Acedido em 20 Fev. 2018]*.

González, M., 2013. *"Nosotros no nos fiamos de nadie" [Em linha] Entrevista El País. Disponível em: https://politica.elpais.com/politica/2013/07/19/actualidad/1374244373_693749.html, [Acedido em 22 Mar. 2018]*.

Gotkowska, J., 2017. *The Cyber and Information Space: a new formation in the Bundeswehr* [Em linha] Disponível em: https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-formation-bundeswehr, [Acedido em 05 Mar. 2018].

Graça, L., 2018. *A criação de Quadro Especial Ciber.* [Entrevista] Lisboa (05 março 2018).

Hathaway, M., 2016. *Germany Cyber Readiness at a Glance* [Em linha] Potomac Institute for Policy Studies. Disponível em: http://www.potomacinstitute.org/images/CRI/CRI_Germany_Profile_PIPS.pdf, [Acedido em 12 Fev. 2018].

IDN, 2013. *Estratégia da Informação e Segurança no Ciberespaço. Investigação conjunta IDN-CESEDEN.* IDN Cadernos N.º 12, Instituto da Defesa Nacional. Lisboa: Imprensa Nacional – Casa da Moeda, SA.

IESM, 2015a. *ACA 018 - Regras de apresentação e referênciação para os trabalhos escritos a realizar no IESM.* Pedrouços: IESM.

IESM, 2015b. *NEP/ACA - 010 - Trabalhos de Investigação.* Pedrouços: IESM.

Jesus, F., 2018. *A Criação de um Quadro Especial Ciber.* [Entrevista] Lisboa (12 Janeiro 2018).

Kilaz Onder e Yanik, I. e. A. e. M., 2014. Manpower Planning and Management in Cyber Defense In: Liaropoulos e Tsihrintzis, ed., 2014. *Proceedings of the 13th European Conference on Cyber Warfare and Security ECCWS-2014,* Pp. 116 - 124. Piraeus: ACPI.

MCCD, 2017. *Jefe del mando de Ciberdefensa: "Si las FFAA pierden el acceso al ciberespacio retrocederían 60 años"* [Em linha] Disponível em: https://www.elperiodico.com/es/politica/20170926/jefe-del-mando-de-ciberdefensa-si-las-ffaa-pierden-el-acceso-al-ciberespacio-retrocederian-60-anos. 60-anos-6311487, [Acedido em 05 Mar. 2018].

MDN, 2013b. *Publicação da Diretiva iniciadora com a Orientação Política para a Ciberdefesa* (Despacho n.º 13692/2013 de 11 de outubro). Lisboa: DR.

MDN, 2014. *Aprovou o Conceito estratégico Militar* (CSD de 30 de julho de 2014) Lisboa: MDN.

MDN, 2017. *Autoriza a assinatura da Nota de adesão ao Centro de Excelência para a Ciberdefesa da OTAN* (Despacho n.º 9762/2017 de 9 de novembro de 2017) Lisboa: DR.

MDN, 2018a. *Aprovou a orientação política do MDN para o novo Ciclo de Planeamento de Defesa Nacional* (DR 79/2018 de 23 de abril). Lisboa: DR.

MDN, 2018b. *Duplo uso, interoperabilidade e "ciberdefesa" são prioridades para investimento - ministro da Defesa.* [Em linha] Disponível em: https://www.lusa.pt/article/24038406/ministro-da-defesa-diz-que-duplo-uso-interoperabilidade-e-ciberdefesa-s%C3%A3o-prioridades-para-investimento. [Acedido em 20 Abr. 2018].

Ministério do Interior Alemão, 2016. *Estratégia de Cibersegurança para a Alemanha.* Berlim: Ministério do Interior Alemão.

Monteiro, A. P., 2017. *Portugal at Forefront of Global Cyber Initiatives* [Em linha] SIGNAL. Disponível em: https://www.afcea.org/content/portugal-forefront-global-cyber-initiatives, [Acedido em 20 Fev. 2018].

Morgado, P., 2018. *A criação de Quadro Especial Ciber.* [Entrevista] Lisboa (09 abril 2018).

Moury, T., 2017. *Exército Brasileiro investe em defesa cibernética* [Em linha] Diálogo Revista Militar Digital. Disponível em: https://dialogo-americas.com/pt/articles/brazilian-army-invests-cyber-defense, (Acedido em 23 Mar. 2018).

NATO, 2016. *Cyber Defence Pledge* [Em linha] OTAN. Disponível em: https://www.nato.int/cps/su/natohq/official_texts_133177.htm, [Acedido em 19 Mar. 2018].

Neves, P. e Correia, F., 2016. *Resposta a Incidentes de Segurança da Informação: uma Abordagem DOTMLPI-I.* Revista Científica sobre Cyberlaw, Número 01. Faculdade de Direito da Universidade de Lisboa. Lisboa: CIJIC.

Neves, *G., 2002. Gestão de Recursos Humanos: Evolução do Problema em Termos dos Conceitos e das Práticas IN: Gestão dos Recursos Humanos: Contextos, Processos e Técnicas.* 2ª ed. Lisboa: Editora RH.

Neves, P., 2015. *Capacidade de resposta a Incidentes de Segurança da Informação no Ciberespaço uma Abordagem DOTMLPI-I.* Tese de Dissertação em Mestrado em Segurança da Informação e Direito no Ciberespaço. Lisboa: FDUL.

Nunes, P., 2012. A Definição de uma Estratégia Nacional de Cibersegurança In: Carriço, A.,2012. *Cibersegurança,* Nação e Defesa N.º 133, IDN. Lisboa: Imprensa Nacional - Casa da Moda S. A.

Nunes, P., 2018. *A criação de Quadro Especial Ciber.*[Entrevista] Lisboa (15 março 2018).

Onemagazine, 2013 . *El Mando Conjunto de Ciberdefensa alcanza la Capacidad Operativa Inicial (IOC)* [Em linha] Onemagazine. Disponível em: http://www.onemagazine.es/noticia/15037/business/el-mando-conjunto-de-ciberdefensa-alcanza-la-capacidad-operativa-inicial-ioc.html,[Acedido em 23 Mar. 2018].

Onemagazine, 2014. *50 Empresas españolas se reúnen con el Mando de Ciberdefensa* [Em linha] Disponível em: http://www.onemagazine.es/noticia/16479/one-hacker-/-noticias/50-empresas-espanolas-se-reunen-con-el-mando-de-ciberdefensa.html, [Acedido em 22 Mar. 2018].

Piña, R., 2017. *El mando militar de la ciberdefensa apoya crear una ciberreserva de 'hackers' sin remuneración económica.* [Em linha] El Mundo. Disponível em: http://www.elmundo.es/espana/2017/11/23/5a16f08eca4741a3198b45f0.html, [Acedido em 20 Fev. 2018].

Pires, F., 2018. *A criação de Quadro Especial Ciber.* [Entrevista] Lisboa (05 abril 2018).

Ribeiro, A., 2018a. Diretiva Estratégica do Estado-Maior General das Forças Armadas 2018/2021. Lisboa. EMGFA

Ribeiro, R., 2002. Recrutamento e Selecção IN: *Gestão dos Recursos Humanos: Contextos, Processos e Técnicas.* 2ª ed. Lisboa: Editora RH.

Ribeiro, S., 2018b. *A criação de Quadro Especial Ciber.*[Entrevista] Lisboa (14 março 2018).

Rodriguez, J., 2018. *A Criação de um Quadro Especial Ciber.*[Entrevista] Lisboa (31 março 2018).

Rolo, M., 2009. *A Qualificação e a Gestão de Competências nas Forças Armadas Desempenho e eficiência nas Forças Armadas.* Trabalho de Investigação Individual do CPOG 2008/2009. IESM. Lisboa: IESM.

Ruiz, M., 2016. *Así se entrenan los soldados españoles para defender el ciberespacio* [Em linha] Disponível em: https://www.eldiario.es/hojaderouter/seguridad/mando_conjunto_de_ciberdefensa-Espana-ejercito-hackers-seguridad_informatica_0_536146646.html, [Acedido em 22 Mar.2018].

Santos, L. e Lima, J., 2016. *Orientações Metodológicas para elaboração de Trabalhos de Investigação.* Cadernos do IESM, 8 ed. Lisboa: Instituto Estudos Superiores Militares.

Santos, L., 2017. *Contributos para uma Estratégia Nacional de Ciberdefesa.*Trabalho de Investigação Individual realizado no âmbito do Curso de Promoção a Oficial General. IUM. Lisboa: IUM.

Santos, L., 2018. *A Criação de um Quadro Especial Ciber.* [Entrevista] Lisboa (05 abril 2018).

Silva, M., 2018. *A Criação de um Quadro Especial Ciber.* [Entrevista] Lisboa (27 março 2018).

Skierka, I., 2018. *Bundeswehr: Cyber security, the German way* [Em linha] Observer Research Foundation. Disponível em: http://www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/, [Acedido em 25 Mar. 2018].

Solms, R. e Niekerk, J., 2013. *From information security to cyber security* [Em linha] Computers & Security 38 (2013) 97 e 102. Disponível em: http://www.profsandhu.com/cs6393_s16/solms-2013.pdf, [Acedido em 05 Mar. 2018].

Stewart, K., 2013. *NPS Student's National Cyber Professionals Association Garners High-Level Attention.* [Em linha] Naval Postgraduate School. Disponível em: https://web.nps.edu/About/News/NPS-Students-National-Cyber-Professionals-Association-Garners-High-Level-Attention.html,. [Acedido em 17 Fev. 2018].

Tanner, L., 2015. *Examining cyber command structures* [Em linha] Disponível em: https://calhoun.nps.edu/bitstream/handle/10945/45262/15Mar_Tanner_Leah.pdf?sequence=1, [Acedido em 25 Mar. 2018].

Thomas, C., 2014. *Human Resources Command stands up Cyber Branch* [Em linha] U.S. ARMY. Disponível em: https://www.army.mil/article/122456/human_resources_command_stands_up_cyber_branch, [Acedido em 12 Fev. 2018].

Torres, A., 2015. *Building a World-Class Security Operations Center: A Roadmap.* SANS Institute. Philadelphia: SANS Institute.

USDoD, 2015. *The Department of Defense Cyber Strategy.* Washington: DoD.

USDoD, 2018. *DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command* [Em linha] U.S. Department of Defense. Disponível em: https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-

elevate-us-cyber-command-to-unified-combatatant-command/. [Acedido em 12 Fev. 2018].

Vinagreiro, J., 2018. *A criação de Quadro Especial Ciber*. [Entrevista] Lisboa (27 março 2018).

Welch, L., 2011. *Cyberspace - The Fifth Operational Domain* [Em linha] Disponível em: https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf, [Acedido em 02 Mar. 2018].

Yannakogeorgos, P. e Geis II, J., 2016. *The human side of cyber conflict : organizing, training, and equipping the Air Force cyber workforce.* University Press, Air Force Research Institute. Maxwell: Air University Press.

Anexo A — Competências de Ciberdefesa do EMGFA

Decreto Regulamentar n.º 13/2015 de 31 de julho

…

Neste enquadramento, o Decreto -Lei n.º 184/2014, de 29 de dezembro, estabelece, no n.º 10 do seu artigo 6.º, que compete ao Chefe do Estado -Maior -General das Forças Armadas definir a organização interna das unidades, estabelecimentos e órgãos do EMGFA, razão pela qual o presente decreto regulamentar estabelece apenas a organização e competências das estruturas principais do EMGFA.

…

CAPÍTULO VII

Direção de Comunicações e Sistemas de Informação

Artigo 40.º

Missão e estrutura

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

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

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

4 — A DIRCSI tem a seguinte estrutura:

a) A Repartição de Coordenação e Integração (RCI);

b) A Repartição de Sistemas de Comunicações (RSC);

c) A Repartição de Sistemas e Tecnologias de Informação (RSTI);

d) A Repartição de Segurança (RSEG);

e) O Centro de Ciberdefesa (CCD);

f) O Serviço de Comunicações e Sistemas de Informação (SCSI);

g) O Centro de Comunicações e Cifra (CCC);

h) O Posto de Controlo.

…

Artigo 45.º

Centro de Ciberdefesa

1 — Ao CCD compete:

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

i) Conduzir operações militares no ciberespaço;

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

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

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

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

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

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

ii) Efetuar a análise forense de ciberincidentes;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 — Aos contratos de aquisição de bens e serviços destinados ao CCD é aplicável o disposto no n.º 3 do artigo 1.º do Decreto - Lei n.º 107/2012, de 18 de maio, alterado pela Lei n.º 83 -C/2013, de 31 de dezembro, e o CCD é considerado um sistema operacional crítico, para efeitos do disposto no n.º 5 da referida disposição legal.

Anexo B — Linhas de Ação para dinamizar a capacidade de CD nacional

Figura 10 - Linhas de Ação para dinamizar a capacidade de CD

Fonte: (Ribeiro, 2018a, p. 28)

Apêndice A — Diferentes abordagens à Ciberdefesa

1. A abordagem dos Estados Unidos da América

A estratégia para operar no ciberespaço, de 2011, do Departamento da Defesa Norte Americano e a sua revisão de 2012, na *Joint Publication on Information Operations* (JP 3-13), refletem o pensamento militar americano que considera o ciberespaço um domínio de guerra. O *U.S. Cyber Command* (USCYBERCOM), que foi criado em 2009 com o propósito defensivo, passou, em agosto de 2017, a um Comando de combate unificado e independente, permitindo melhorar a gestão dos recursos Ciber e a interoperabilidade (USDoD, 2018).

Trata-se de um comando subordinado do *U.S. Strategic Command*, composto por várias componentes militares e serviços, que garantem as suas capacidades (figura 8).

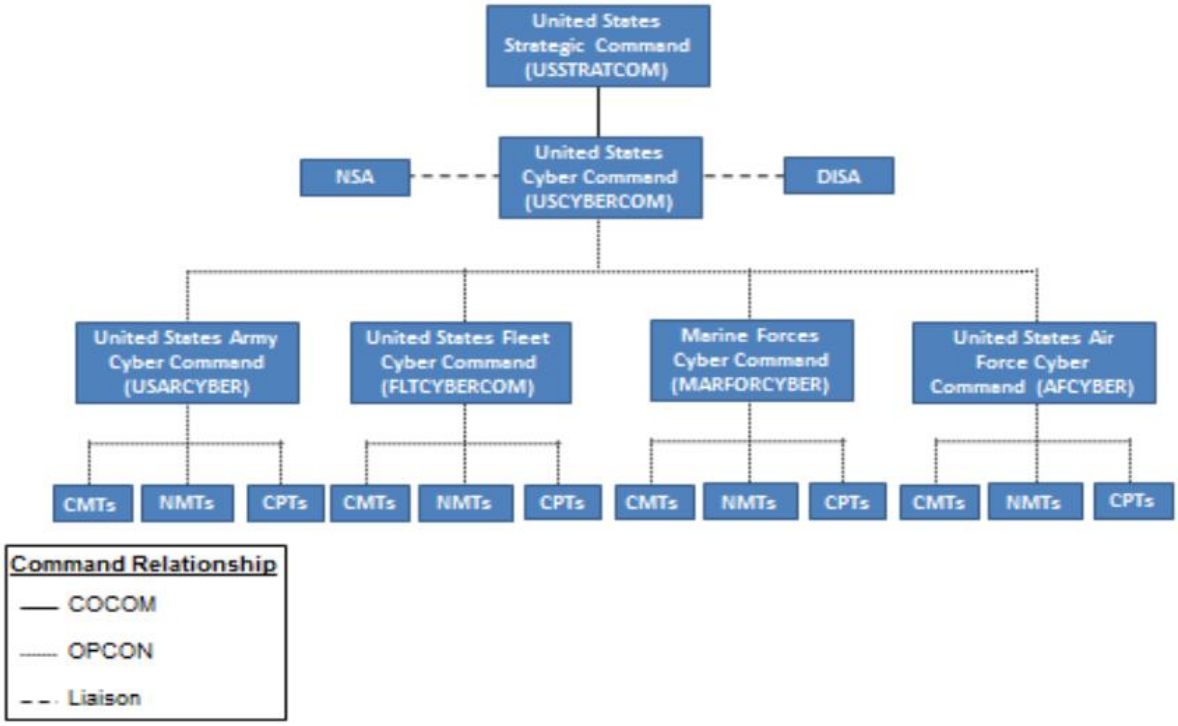

Figura 11 - Estrutura do USCIBERCOM
Fonte: (Tanner, 2015, p. 26)

Quando estiver totalmente operacional, este comando contará com 6200 pessoas, entre militares, civis e pessoal de apoio contratado, organizado em 133 equipas, sendo que todas as equipas já alcançaram a capacidade mínima de operabilidade (USDoD, 2015).

Trata-se de um grande desafio para a GRH, o que levou o Exército americano a estabelecer um ramo Ciber provisional, para garantir a gestão de carreira e o seu desenvolvimento de forma estável, de modo a atingir a profundidade exigida nesta área altamente especializada (Thomas, 2014).

2. A abordagem da República Federativa do Brasil

O Brasil evoluiu a sua estrutura Ciber numa ótica em que um dos ramos presta serviço aos outros ramos, com provas dadas de sucesso que ajudaram à sua maturação, nomeadamente o Campeonato do Mundo de Futebol de 2014, e os Jogos Olímpicos em 2016 (Moury, 2017).

Depois da aprovação em 2008 da Estratégia Nacional de Defesa, o EB ficou responsável pela coordenação e integração do Setor Cibernético. Seguidamente, em 2010, foi criado o Centro de Defesa Cibernética (CDCiber), em 2014, foi aprovada a Doutrina Militar de Defesa Cibernética e, em 2016, foram oficialmente criados o Comando de

Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber) (Carneiro, 2016, p. 20 a 22).

O ComDCiber é o órgão responsável pela coordenação e integração das atividades Ciber na DN e conta com servidores militares e civis altamente especializados. Os militares da Marinha e da FA ficam à disposição do Exército pelo tempo máximo de quatro anos. Desenvolve as suas atividades nas áreas dos RH, Doutrina, Ciência e Tecnologia, Informações e Operações (Carneiro, 2016, p. 25).

O ComDCiber é organizado seguintes estruturas (figura 9): (i) Comando, Estado-Maior Pessoal e Auxiliares; (ii) Gabinete; (iii) Estado-Maior Conjunto; (iv) Departamento de Gestão e Ensino com Núcleo da Escola Nacional de Defesa Cibernética, Divisão de Gestão de Pessoal, Divisão de Projetos, Divisão de Relações Institucionais;(v) Centro de Defesa Cibernética (figura 9).

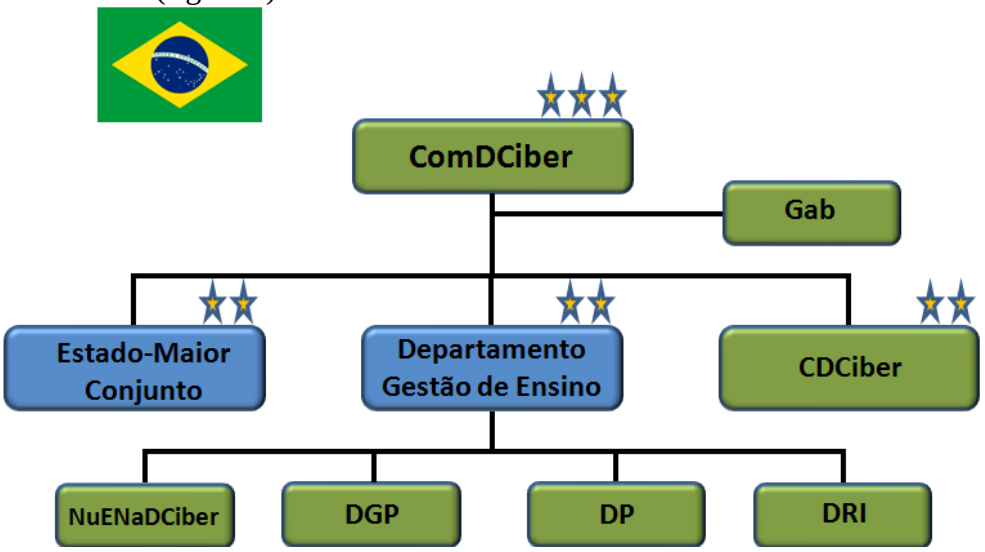

Figura 12 - Estrutura do ComDCiber
Fonte: Adaptado de (Carneiro, 2016, p. 27)

Apesar de ser uma estrutura que está debaixo do EB, é comandado por oficiais generais da Marinha e da FA. Além do trabalho conjunto realizado no ComDCiber, cada ramo possui equipas ou Centros de Tratamento de Incidentes de Rede (CTIR) próprios (Moury, 2017). De salientar, também, resultante da necessidade de se capacitar RH na área cibernética, a criação da ENaDCiber, de caráter dual, civil e militar, considerada como centro polarizador de ensino e pesquisa da Defesa Cibernética Nacional (Carneiro, 2016, p. 27).

3. A abordagem da República Federal da Alemanha

A Estratégia de Cibersegurança para a Alemanha de 2016 (Ministério do Interior Alemão, 2016), atribuiu ao Ministério Federal do Interior a responsabilidade pela CS na Alemanha e, ao Conselho Nacional de Ciber Segurança, a coordenação técnica da defesa e da política Ciber na Alemanha (Hathaway, 2016, p. 15).

Neste contexto, o novo plano de segurança Ciber, "*White Paper On German Security Policy and the Bundeswehr*", de 2016, colocou os riscos cibernéticos no nível superior das ameaças nacionais e estabeleceu o *Kommando Cyber- und Informationsraum* (Kdo CIR) (figura 10) nas FFAA. O Kdo CIR, com a ativação do sexto ramo das FFAA alemãs, ficou operacional em abril de 2017. É comandando, a partir de Bona, por um Tenente-general e tem a missão de segurança das TIC, informações militares, informação geoestratégica e comunicação operativas (Skierka, 2018, p. 3).

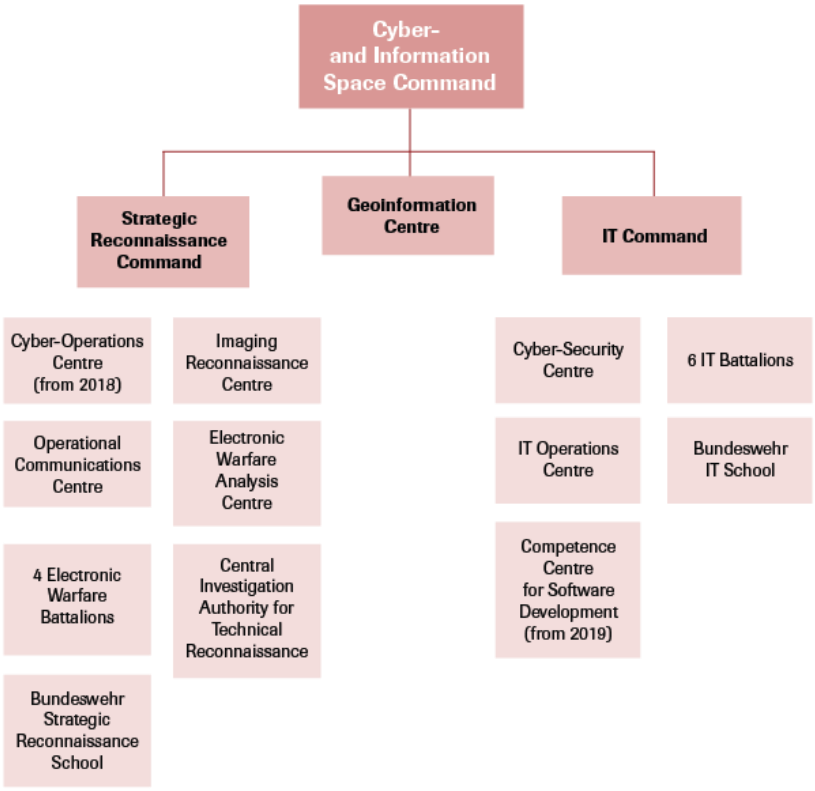

Figura 13 - Estrutura do Kdo CIR
Fonte: (Gotkowska, 2017)

Espera-se que, em 2021, este novo comando tenha as suas novas instalações concluídas, estimando-se que venha a ter 13.500 efetivos, entre militares e civis. As FFAA adotaram uma maior flexibilidade. Lançaram uma campanha de recrutamento em larga escala, institucionalizaram novos percursos de carreira, o pagamento de salários mais elevados, garantias de formação aos novos recrutas e possibilidade de treino avançado. Foi, inclusivamente, criado um Mestrado em Cibersegurança ministrado na Universidade das FFAA, para 70 novos formandos anuais (Skierka, 2018, pp. 3-4).

4. Síntese conclusiva

As abordagens e as soluções encontradas pelos diferentes países refletem a importância atribuída à CD e à SI, como uma Componente a par das tradicionais. Os EUA e a maioria dos países ocidentais, tais como Reino Unido, França e Holanda e Espanha, optaram pela constituição de um CC, em dimensão proporcional às suas FFAA. A Alemanha diferencia-se por ter constituído o sexto ramo das suas FFAA.

Transversalmente às situações abordadas, constatamos que todos prosseguem, como documentos fundamentais, as estratégias nacionais de Cibersegurança. Trata-se de uma capacidade em crescendo, apoiadas em estruturas dedicadas, que vão maturando à medida das necessidades. A maior dificuldade com que se têm deparado, é a capacitação dos RH com formação e treino adequados, pelo que, para além da contratação de funcionários civis, constituíram estabelecimentos de ensino específicos.

O Brasil, também, constituiu um CC, diferenciando-se, porém, na forma como o fez, tendo atribuído essa tarefa ao EB.

Estas estruturas têm influência direta na GRH e, a que melhor garante uma GRH em pleno, é a solução adotada pela Alemanha, porque tem dimensão suficiente, cerca de 13500 elementos, com uma natural progressão na carreira, comportando todas as categorias, todos os postos e encaixando os mecanismos de GRH.

Apêndice B — Modelo de análise

Quadro 2 - Modelo de análise

Objetivo geral			
Apurar qual o modelo de GRH que melhor se adequa aos militares especializados em CD e SI das FFAA, de forma a obter ganhos operacionais nesta capacidade.			
Objetivos específicos			
OE1: Identificar o impacto que a GRH tem, atualmente, na capacidade operacional de CD das FFAA.			
OE2: Caraterizar o modelo de GRH empregue na capacidade de CD nas FFAA de um país da OTAN.			
OE3: Identificar as medidas que podem ser implementadas na GRH Ciber das FFAA.			
Questão Central			
Como poderá ser otimizada a GRH Ciber nas estruturas Ciber das FFAA?			
Questão Derivadas	**Conceitos**	**Dimensões**	**Indicadores**
QD1: Qual o impacto da atual GRH Ciber na capacidade operacional de CD das FFAA?	GRH	Seleção e Recrutamento	Militares
			Civis
		Formação e Treino	Formação Base
			Especialização
QD2: Qual o modelo de GRH empregue no *Mando Conjunto de Ciberdefensa* das FFAA do Reino de Espanha?			Treino
			Experiência
		Retenção	Gestão diferenciada
			Desenvolvimento pessoal
QD3: Quais as medidas que ao nível da GRH Ciber, podem ser implementadas com vantagens para a capacidade de CD das FFAA?			Carreira
			Tempo de permanência
			Remuneração

Fonte: (Autor, 2018)

Apêndice C — Impacto da GRH na capacidade de Ciberdefesa do CCD

Tabela 7 - Impacto da GRH na capacidade de CD do CCD

ORGANIZAÇÃO		IMPACTO		
		+	N	-
Equipas	O reduzido número de militares afetos ao CCD inviabiliza a constituição de equipas, não abrange todas as funções e restringe-se à SI.			-
Processos	Os processos de resposta a incidentes adquirem-se com treino, coordenação e experiência.		N	
Gestão	A responsabilidade da prossecução da estratégia é da responsabilidade do seu chefe.			-
TREINO				
Formação	Para ingresso no CCD estão definidos requisitos mínimos de formação. É necessário a implementação de um plano de formação específica, comum às FFAA.			-
Treino	Portugal lidera o MNCDE&T e para além disso participa em exercícios no âmbito da OTAN e em exercícios nacionais no âmbito da CS.		N	
Experiência	A experiência adquirida no dia-a-dia também deve ser valorizada, dependente do tempo de permanência.		N	
LIDERANÇA				
Carreira	Os líderes devem estar no topo da carreira Ciber, mas como o CCD é muito recente ainda não é possível. Permite aos oficiais desempenhar várias funções ao longo da carreira.		N	
Permanência	Dois anos não permitem ao líder desenvolver a sua estratégia.			-
Cultura Ciber	Os líderes devem promover a coesão da equipa, a cultura cibernética e construir atratividade.			-
PESSOAL				
QO	Os QO devem ser adequados aos problemas identificados e abrangentes com oficiais, sargentos e praças, para as diferentes funções.			-
Alimentação	O CCD é alimentado com RH especializados dos ramos em regime de comissão de serviço.		N	
Gestão	Os militares do CCD não estão a coberto de uma GRH diferenciada.			-
Civis	O CCD não tem civis, mas estes garantem maior permanência e podem colmatar a falta de militares.			-
Retenção	Tempo - permanência de 3+2 anos.		N	
	Carreira - sujeitos às mesmas regras, com cursos e requisitos de promoção iguais aos restantes militares.			-
	Carreira Técnica – EMFAR prevê carreira horizontal, mas sem regulamentação.			-
	Remuneração - não existe qualquer tipo de aumento remuneratório.			-
	Mercado de Trabalho – saída dos melhores elementos			-

Fonte: (Autor, 2018)

Apêndice D — Impacto da GRH na capacidade de Ciberdefesa do MCCD

Tabela 8 - Impacto da GRH na capacidade de CD do MCCD

ORGANIZAÇÃO		IMPACTO		
		+	N	-
Equipas	Desde a sua IOC que o MCCD tem vindo a aumentar o número de militares, para cumprir todas as funções. Está dividido em Estado-maior, Operações e Apoio.		N	
Processos	Minimamente operacional desde setembro de 2013, já teve tempo de adquirir os processos necessários.	+		
Gestão	Desde julho de 2013 que o Comandante do MCCD se mantém, permitindo uma implementação duradoura.	+		
TREINO				
Formação	As FFAA espanholas implementaram um plano de formação específica, com cursos básicos, avançados e de especialidade, e a CD está incluída na formação base das academias militares.	+		
Treino	Participação em exercícios de CD no âmbito nacional e da OTAN. Participa no planeamento e execução de exercícios operacionais.	+		
Experiência	A funcionar operacionalmente desde setembro de 2013, adquiriu um determinado nível de experiência.		N	
LIDERANÇA				
Carreira	O General Medina é formado em transmissões e EW, tem especializações em telecomunicações.	+		
Permanência	Mantêm-se na função desde julho de 2013, o que lhe permite desenvolver a sua estratégia.	+		
Cultura Ciber	Os líderes devem promover a coesão da equipa, a cultura cibernética e construir atratividade.		N	
PESSOAL				
QO	Com um QO planeado para 70 elementos, abrange oficiais, sargentos e praças, e elementos Civis.		N	
Alimentação	É alimentado com RH dos ramos, com ou sem experiência, em comissão de serviço e Civis.	+		
Gestão	Os militares do MCCD não estão a coberto de uma GRH diferenciada.			-
Civis	Dos cerca de 70 elementos planeados contará com 21 funcionários civis. As restrições orçamentais não têm permitido a contratação desejável.		N	
Retenção	Tempo - permanência mínima de 2 anos.			-
	Carreira - sujeitos às mesmas regras, com cursos e requisitos de promoção iguais aos restantes militares.			-
	Nas FFAA espanholas não está prevista Carreira Técnica opcional.			-
	Remuneração - não existe qualquer tipo de aumento remuneratório.			-
	Mercado de Trabalho – forte assédio aos melhores elementos. Obrigatoriedade de permanência de 2 anos.			-

Fonte: (Autor, 2018)

Apêndice E — Guião da entrevista

Guião da entrevista

Identificação:

Função:

Para responder às orientações políticas da Segurança Nacional e Defesa, foi criado em 2015, na estrutura do EMGFA, o Centro de Ciberdefesa (CCD), que entre outras atividades, coordena o trabalho cooperativo da *Computer Incident Response Capability* (CIRC), nos três ramos das Forças Armadas (FFAA). Para além disso o CCD é alimentado com os Recursos Humanos (RH) especializados dos ramos.

Face aos escassos RH e as dificuldades sentidas na sua gestão, foi colocada a questão da pertinência da criação de um **Quadro Especial (QE) Ciber**, garantindo-se as necessidades das FFAA, tendo em conta as dificuldades de recrutamento, formação, treino e retenção através de uma eficaz gestão de carreira, conseguindo-se desta forma ir ao encontro das espectativas dos militares e da instituição.

Este novo QE a ser aprovado, seria distribuído por categorias e postos, garantindo-se pessoal com diferentes níveis de especialização, para as diferentes funções a desempenhar (n.º 4, do art.º 166 do EMFAR - DL 90/2015, de 29 de maio).Face ao exposto:

1. Considerando as Orientações Políticas para a Ciberdefesa (Despacho n.º 13692/13, de 11 de outubro de 2013, do MDN) e restante legislação enquadradora da Ciberdefesa e da Segurança da Informação, considera os RH afetos a esta atividade suficientes para garantir um nível operacional satisfatório?
2. Na lógica da questão anterior, em que aspetos considera haver melhorias a implementar ao nível da gestão destes RH. Indique quais e porquê?
3. Na conjuntura atual e na ótica de uma GRH mais eficaz, faz sentido a criação de um novo QE Ciber (Classe/Arma/Especialidade) nas FFAA? Argumente a sua resposta.
4. Uma forma de mitigar a falta destes RH especializados, é a contratação de especialistas civis. Quais as vantagens e desvantagens desta opção?
5. Não sendo possível a criação deste QE Ciber que medidas podem ser adotadas, para melhorar a retenção destes elementos na função?

Luis Miguel Gomes Ferreira

Maj GNR

Apêndice F — Excertos das respostas dos entrevistados

Quadro 3 – Excertos e segmentos de resposta por entrevistado

Entrevistado	Excerto da resposta	Segmento
Pergunta 1	Considerando as Orientações Politicas para a Ciberdefesa (Despacho n.º 13692/13, de 11 de outubro de 2013, do MDN) e restante legislação enquadradora da Ciberdefesa e da Segurança da Informação, considera os RH afetos a esta atividade suficientes para garantir um nível operacional satisfatório?	
1	*"Não, os atuais RH são claramente insuficientes para todas as tarefas operacionais e de suporte de estado-maior que neste momento recaem sobre o CCD."*	**A.1.2**
2	*"Não têm porque para já não têm pessoal para isso não é, mas haverá o tempo em que se houver uma decisão do país e do estado para que isso aconteça, tem que acontecer tem que se gerar os meios …"* *"Isso infelizmente acontece nos vários ramos e vai acontecer cada vez mais […] mas o que o sistema tem de garantir é que as saídas sejam iguais às entradas no mínimo."*	**A.1.2** **A.1.3**
3	*"… nesta primeira fase de implementação os meios que existem são suficientes, agora para cumprir o que o CCD deve ser e as missões que lhe estão incumbidas, tanto na LO do EMGFA como na ENSC e nas OPC, não claramente que ficam muito aquém, é preciso fazer a evolução, mas essa evolução é difícil…"* *"… e depois de se lhes dar formação, são excecionalmente caros, os dois melhores operadores do Exército saíram em 2015*	**A.1.2** **A.1.3**
4	*"tendo em conta que esta realidade é uma realidade relativamente recente, as espectativas ainda estão em fase de avaliação. No que ao CCD diz respeito, este terá de crescer no sentido de garantir uma maior capacidade de atuação, de resposta aos desígnios nacionais"*	**A.1.2**
5	*"… a DP não é o órgão que se deva pronunciar, em termos operacionais, sobre se uma determinada unidade tem ou não uma lotação adequada às suas atribuições e competências, como é o caso do CCD do EMGFA,"*	**A.1.4**
6	*"Tomando como referência apenas o universo mais restrito do núcleo CIRC, claramente não são suficientes, sobretudo em quantidade, mas também em qualificação (que forçosamente tem de acompanhar a evolução em quantidade)."*	**A.1.2**
7	*" o Departamento de CD e SI tem um Núcleo de Operações de CD que opera permanentemente para monitorizar a segurança da rede de dados do Exército, e é a partir deste núcleo que se constitui o Núcleo CIRC do Exército que tem um QO específico […] este Núcleo CIRC do Exército só se constitui em caso de necessidade, em situação de crise, e quando eu formo este núcleo deixo de ter pessoas a funcionar no Núcleo de Operações de CD, e depois é partir deste núcleo de Operação de CD que sai a componente tática …"* *" … estamos a perder oficiais, a meterem o papel para saírem, a apetência das empresas civis para esta área é muito grande …"*	**A.1.2** **A.1.3**

8	*"Não. No caso concreto do Exército, até ao momento não foi possível preencher a totalidade dos RH previstos em QO do Exército para estas áreas"* *"…, o que temos assistido, no caso concreto do Exército, é a saída de militares do QP para empresas civis, nacionais e estrangeiras, onde os salários chegam a ser seis vezes superiores ao de um oficial superior."*	**A.1.2** **A.1.3**
9	*"…, considero que os RH afetos a esta atividade não devem ser suficientes para garantir todos os militares especializados necessários para cobrir a grande amplitude de tarefas que os objetivos da política de ciberdefesa acarretam"* *", … devido às crescentes necessidades de pessoal para as áreas de cibersegurança das empresas civis, tem vindo a assistir-se a um elevado assédio por parte do mercado civil em relação ao militares especializados na Ciberdefesa"*	**A.1.2** **A.1.3**
10	*"Dada a importância crescente dos Sistemas de Comunicações e Sistemas de Informação no contexto das atividades levadas a cabo no âmbito das Forças Armadas, considero que os RH afetos, atualmente, às áreas da Ciberdefesa e da Segurança da Informação, são insuficientes para dar resposta a todas as solicitações."*	**A.1.2**

Pergunta 2	Na lógica da questão anterior, em que aspetos considera haver melhorias a implementar ao nível da gestão destes RH. Indique quais e porquê?	
1	*"… uma vez que os militares têm uma maior rotatividade fazendo com que o conhecimento adquirido se perca quando acabam as comissões de serviço."* *"…, não se trata de melhorias a implementar na gestão dos RH, mas sim de uma reestruturação do próprio QO do CCD."* *"… os elementos que se venham apresentar para prestar serviço nesta área já venham com a formação de base necessária para o desempenho das funções, …"*	**A.2.2** **A.2.5** **A.2.6**
2	*"… e que eles vejam nesta área nesta permanência como uma área de grande valor para o futuro profissional deles, porque o mercado vai absorve los imediatamente, tem que haver é um acordo, tipo 8 anos de serviço ali …"* *"O QO de 10 é manifestamente pequenino. É insuficiente em número e o problema não é só o número tem a ver com as capacidades efetivas …"*	**A.2.2** **A.2.6**
3	*"…para esta parte julgo que a GRH está bem feita […] agora a gestão destes RH noutra perspetiva, do que deveria ser já o CCD, e que também não deveria ser CCD, deveria já ter outra nome, para corresponder a outra função, essa é outra questão…"*	**A.2.5**
4	*"Os ramos não têm o pessoal desejado, e esta situação potencia eventuais implicações na sustentação do CCD"* *"… a não existência de RH capacitados para esta área."*	**A.2.5** **A.2.6**
5	*"… havendo por parte da Direção de Pessoal uma tentativa de compromisso para que os mesmos militares possam desempenhar as*	**A.2.2** **A.2.5**

	suas funções por períodos não inferiores a 5 anos, no sentido de garantir alguma estabilidade …" *"…, promover e garantir formação adequada a novos elementos, possibilitando assim, as necessárias rendições."* *"… formar o pessoal e alocá-los de acordo com as necessidades definidas e estabilidades superiormente pelas entidades competentes, que criam as necessidades, as unidades e definem as lotações e requisitos dos cargos."*	**A.2.6**
6	*"Há necessidade de reforçar em quantidade (também acompanhada de qualificação) […] há também fragilidades ao nível das competências jurídicas especializadas em matérias Ciber"* *"Há necessidade de reforçar em quantidade (também acompanhada de qualificação) sobretudo nas funções de monitores de incidentes, gestores de incidentes e analistas forenses (ainda no universo mais restrito do núcleo CIRC)."* *"Torna-se, portanto, necessário encontrar outro perfil de carreira para este pessoal que garanta tempos muito superiores de permanência nestas funções."*	**A.2.2** **A.2.5** **A.2.6**
7	*"Não devemos ter uma capacidade isolada […], exércitos de pequena dimensão como é o caso de Portugal e da Marinha e FA, não se justifica termos uma capacidade, ao nível de estruturas de pessoal, isolada"* *"…, nós temos que dar experiência numa 1ª fase, na componente de rede […] para depois de aprenderem isso começarem a trabalhar especificamente na CD, portanto há aqui vários passos na formação que é a aprendizagem ao longo da vida, que as pessoas têm de passar, para serem bons especialistas em CD …"*	**A.2.5** **A.2.6**
8	*"a GRH em áreas tão sensíveis, […]como são as comunicações e a CD […], não pode ser feita à imagem do que é feito com as restantes áreas da Defesa."* *"…, não pode ser dada formação dispendiosa a um militar e este passados alguns meses ou poucos anos é deslocado."* *"… existem alguns mecanismos que podem ser utilizados como é o caso da inamovibilidade por um período de tempo relacionado com as funções, …"* *"…, a elevada rotatividade em determinados postos para dar condições de promoção como é o caso de comando de companhia no posto de capitão para a promoção a oficial superior ou comando de oficial superior para as condições de promoção a Coronel."* *"… inamovibilidade por um período de tempo relacionado com as funções, experiência e formação exigida, salvaguardando as condições de progressão na carreira através da equivalência de funções de comando …"* *"…, a nomeação de militares para desempenhar funções nestas áreas deverá ter em conta o percurso profissional e a experiência adquirida ao longo do tempo"* *"… a definição do número de vagas para oficiais e sargentos do Exército , deverá ter em conta as necessidades de RH para estas áreas, o que não se tem verificado"*	**A.2.1** **A.2.2** **A.2.3** **A.2.4** **A.2.5**

9	*"… logo ao nível genético, as admissões de pessoal, para as Classes/Armas/Especialidades concernentes, devem reflectir, em articulação conjunta, as necessidades específicas para a Ciberdefesa"* *"… considero que devem existir mecanismos de retenção específicos ("tailored") que permitam rentabilizar os custos dos cursos de formação destes militares e garantir a permanência deste pessoal na área da ciberdefesa durante os anos considerados adequados."*	**A.2.2** **A.2.5**
10	*"A retenção dos RH já qualificados, tendo em conta o nível de especialização necessário relativamente a algumas tarefas, bem como os recursos necessários tendo em vista essa especialização."* *"Aumento dos RH envolvidos, em exclusividade, às tarefas relacionadas com a Ciberdefesa e a Cibersegurança nas Forças Armadas."* *"A seleção e a qualificação dos RH mais adequados àquelas funções."*	**A.2.2** **A.2.5** **A.2.6**

Pergunta 3	Na conjuntura atual e na ótica de uma GRH mais eficaz, faz sentido a criação de um novo QE Ciber (Classe/Arma/Especialidade) nas FFAA? Argumente a sua resposta.	
1	*"Na conjuntura atual […],eu não favoreço nesta altura, não temos gente suficiente sequer para constituir um quadro …"*	**A.3.2**
2	*"… a criação de um ramo ou de uma estrutura de especialidade, não digo um ramo logo assim de início mas a minha visão é que nos próximos anos temos que ter pelo menos um comando semelhante ao Cmd das OpEsp."* *"… a especialização é a lógica da especialização, na minha opinião faria muito mais sentido em termos de pragmatismo encararmos isto desta forma porque neste momento pulverizamos o pouco que temos é o contrário que os outros estão a fazer, …"*	**A.3.2** **A.3.4**
3	*"… não, julgo que não temos capacidade para isso, o que temos é capacidade de dar uma especialização a partir dos postos mais baixos, …"*	**A.3.2** **A.3.4**
4	*"é uma solução adotada internacionalmente, destacando-se a Alemanha que criou um sexto ramo. […] Neste momento não tenho condições de afirmar qual a melhor solução."*	**A.3.3**
5	*"Na minha ótica não faz sentido criar uma classe ou mais uma classe para esta área tão específica e particular, talvez no máximo uma especialização."*	**A.3.2** **A.3.4**
6	*"…, a criação de um QE Ciber afigura-se o caminho mais provável, a prazo, eventualmente."* *"A Marinha já teve um conjunto de cursos, nos seus planos de formação, que possibilitavam uma especialização em "informática", para os quais podiam concorrer as três categorias (Of, Sarg. e praças). Não correspondendo a uma classe ou sequer sub-classe, o nível de especialização era assinalável …"*	**A.3.2** **A.3.4**

7	*"..., um país como nós não justifica essa capacidade independente, a componente tática e mesmo a territorial, que pode operar permanentemente, são pequenos núcleos de pequena dimensão que não justifica um QE só para a CD ..."* *"... no Exército e na área de transmissões, estamos bem organizados e temos conseguido alimentar e criar especialistas desta forma, [...] depois estes especialistas que se tornam especialistas e que nós entendemos que eles têm capacidade nesta área, damos-lhe uma formação adicional de CD."*	**A.3.2** **A.3.4**
8	*"com a atual estrutura criada, este QE não faz qualquer sentido porque não é possível criar uma carreira para os RH afetos a ela"*	**A.3.2**
9	*"Mesmo partindo do pressuposto que os militares em causa fazem toda a sua carreira na ciberdefesa, julgo que o conceito de subclasse/especialidade/subespecialidade fará mais sentido do que um novo QE."* *"... a opção por uma subclasse/especialidade/subespecialidade Ciber permitirá uma maior riqueza de "recrutamento" para além de salvaguardar melhores opções/possibilidades de carreira para os militares."*	**A.3.2** **A.3.4**
10	*"Merece análise e reflexão a criação de um Quadro Especial Ciber. Na minha opinião não se justifica a criação de tal Quadro."*	**A.3.2**

Pergunta 4	Uma forma de mitigar a falta destes RH especializados, é a contratação de especialistas civis. Quais as vantagens e desvantagens desta opção?	
1	*"permitiria ainda o conhecimento especializado e atualizado, menores necessidade de formação, experiência técnica, desempenho de funções se m constrangimentos administrativos normalmente associados à carreira militar;"* *"permitiria ainda [...],períodos alargados de permanência em funções específicas da área, melhorando o conhecimento e capacidade técnica pelo acumular de experiência."* *"..., a contratação de civis poderá ter vantagens, pois garantiria uma maior continuidade em termos de conhecimento adquirido, isto uma vez que os militares têm maior rotatividade ..."* *"..., uma cultura diferente da militar que poderá criar alguns conflitos, o risco de exfiltração de informação sensível e o potencial aumento do stress psicológico em operações reais."* *"... tem desvantagens decorrentes de recursos humanos que se regem por estatutos e regras diferentes dos militares, nomeadamente no que se refere a horários, a carreiras e a flexibilidade de empenhamento em cargos e funções [...] ainda referir os custos de contratação e manutenção dos recursos, ..."*	**A.4.1** **A.4.2** **A.4.3** **A.4.4** **A.4.5**
2	*"Não devemos pensar em civis e militares, devemos pensar em competências e capacidades, [...] agora componentes técnicas, não há cores na técnica nem nas competências, de todo, nós temos que juntar todas as competências que conseguir-mos porque se houver uma crise a sério, nós temos de ter capacidade de ativar toda a massa cinzenta*	**A.4.3**

	que estiver disponível,"	
3	*"Só há hipótese de edificar uma capacidade de CD com civis, […] porque o tempo de permanência o tempo médio, para um indivíduo que saiba muito de redes e que se mexa bem no ciberespaço, para ele se tornar, um bom operador Ciber, estatisticamente são necessários 5 anos …, ora isto é completamente incompatível com a nossa gestão de carreiras"* *"… os civis como operadores do ciberespaço, os fighters, os guerreiros do ciberespaço, os cyberspace warriors, têm que ser maioritariamente civis, principalmente ao nível operacional e estratégico da CD, com os militares, qual é o papel dos militares? É gerir as equipas, estabelecer os procedimentos do EM e definir os objetivos e as medidas de avaliação de desempenho, porque os covis não podem decidir onde é que devem atacar e onde é que devem defender, os civis têm é que operar tecnicamente…"* *"…, só tem um problema, estes operadores não são baratos e depois de se lhes dar formação, são excecionalmente caros […] os melhores operadores vão-se embora, …"*	**A.4.1** **A.4.2** **A.4.5**
4	*"é um aspeto a considerar, particularmente pela sustentação em tempo que asseguram"*	**A.4.1**
5	*"É um facto que a contratação pontual de civis para a área da defesa poderá mitigar alguma falta de RH com formação adequada, provendo alguns cargos de cariz mais técnico especifico, em áreas onde haja maior dificuldade em recrutar/formar."* *", … não se vendo assim necessidade de aumentar ou reforçar o Mapa de Pessoal Civil da Marinha na área da Informática e áreas afins."*	**A.4.2** **A.4.6**
6	*"A existência de especialistas civis, cujos ciclos de gestão/rendição são normalmente muito mais longos do que o pessoal militar, confere alguma estabilidade ao nível dos conhecimentos, competências e perícias que ficam na organização."* *"Teoricamente a contratação de especialistas civis, com a criação de canais que permitam a admissão, mas também a saída, de RH na organização permitiria responder aos "picos" e às "cavas" de solicitação que as UEO de TIC estão frequentemente sujeitas."* *"Contudo, as circunstâncias atuais do mercado laboral (com uma procura que, generalizadamente, excede a oferta de pessoal competente nas áreas TIC), só permitirão tornar esta opção viável, de modo continuado no tempo, caso as condições oferecidas a estes especialistas civis se comparem com as condições de mercado."*	**A.4.1** **A.4.2** **A.4.5**
7	*" faz sentido porque a especificidade desta área e a evolução tecnologia a que ela está sujeita, não se compadece com a rotação a curto prazo dos militares que estão a trabalhar lá,[…] e estes civis no CCD podiam dar alguma continuidade, porque os militares não têm possibilidade de dar essa continuidade"* *"é difícil manter civis cá dentro, tendo em conta os níveis remuneratórios que praticamos é impossível manter técnicos cá dentro"*	**A.4.1** **A.4.2** **A.4.5**
8	*"A vantagem mais óbvia é a possibilidade de uma maior*	**A.4.1**

	permanência nas funções e consequente mitigação da ausência de militares em áreas mais técnicas." *"Isto traduz-se numa maior especialização nestas áreas do conhecimento"* *"Uma desvantagem que vejo é a limitação de emprego de civis em operações militares."* *"Este poderá ser sempre um risco que este tipo de recrutamento pode trazer, ou seja um investimento elevado com pouco retorno."*	**A.4.2** **A.4.3** **A.4.4** **A.4.5**
9	*"A contratação de especialistas civis tem a vantagem de garantir uma maior estabilidade do quadro de pessoal afeto à CD assim como as de manter a experiência, o histórico e o "know how" naquela área."* *"… a desvantagem prender-se-á com a carreira pouco aliciante dos trabalhadores civis na administração publica, o que dificultará o recrutamento e tornará os especialistas civis alvo prioritário do assédio das empresas."*	**A.4.1** **A.4.5**
10	*"Existem vantagens na contratação de especialistas civis como reforço de equipas nas áreas de Ciberdefesa e de Cibersegurança, nomeadamente, a inerente estabilidade do ponto de vista de colocação."* *"As desvantagens da contratação destes especialistas passam pela inexistência de um vínculo militar, o que pode comprometer as suas funções em situação de crise."*	**A.4.1** **A.4.2** **A.4.4**

Pergunta 5	Não sendo possível a criação deste QE Ciber que medidas podem ser adotadas, para melhorar a retenção destes elementos na função?	
1	*"… que os elementos que se venham a apresentar para prestar serviço nesta área já venham com a formação de base necessária para o desempenho das funções, …"* *"…, um aspeto a considerar seria uma janela temporal alargada para desempenho de funções, com a possibilidade de evolução nas funções dentro dos respetivos organismos …"* *"Pode ainda considerar-se a adoção de medidas que aumentem o bem-estar e satisfação profissional dos militares, tais como a formação especializada e de qualidade, garantia de continuidade temporal em funções no CCD e CIRC's, relacionadas com o percurso formativo e de especialização."*	**A.5.2** **A.5.4** **A.5.5**
2	*"… precisamos de investir é no conhecimento das pessoas, no RH, …"* *"…, muitas vezes as pessoas falam do dinheiro, atratividade económica, tem o seu impacto, agora não é o único fator."* *"… são do Exército, FA e Marinha que estão lá para uma comissão de serviço, eles a seguir têm de voltar à Marinha ao Exército e à FA, agora há-de haver um momento no tempo em que se percebe que esta rotação, não só não é aceitável, sob o ponto de vista da capacidade como é completamente ilógica, aquele indivíduo é especialista naquela zona, se lhe vão dar uma tarefa menor a seguir …"* *"… tem que haver um contrato com os mais jovens, os recém*	**A.5.2** **A.5.3** **A.5.4** **A.5.5** **A.5.6**

	formados que chegam das faculdades etc, em que se lhes ofereça a oportunidade, uns pacotes de formação que não são baratos a maior parte das vezes que são atrativos para o futuro deles, e que eles vejam nesta área, nesta permanência, uma área de grande valor para o futuro profissional deles, porque o mercado vai absorve-los imediatamente " *"A sensação ou a noção que se está a trabalhar numa área de ponta é um atrativo para qualquer pessoa que tenha vontade de fazer e de aprender,"*	
3	*"É melhorar, é começar por sensibilizar os ramos para uma formação precoce, uma especialização precoce, […] para oficiais, sargentos e praças […] por exemplo na área das transmissões passarem pelo Regimento de Transmissões no Porto, damos a parte de formação toda CISCO, que não é CD mas é no fundo para conhecerem a plataforma onde depois vão ter de puxar pela cabeça para atuar, …"* *"… e praças, especialmente agora neste novo quadro dos contratos de longa duração e com possibilidades de passar por exemplo … eu vejo isto, nós vamos dar formação aos praças, eles como têm aquele problema de ao final dos 18 anos, ou agora aos seis anos, estão para se ir embora não é, portanto, criar uns números cláusulos para que eles entrassem como civis para dentro das FFAA, isto seria uma boa saída …"*	**A.5.2** **A.5.6**
4	*"… passa por haver uma formação de base tecnológica igual nos três ramos. No mínimo falaríamos de um mínimo denominador comum."*	**A.5.2**
5	*"… deverá haver um esforço para, por um lado, alocar ou colocar as pessoas com a formação adequada a desempenhar funções nas áreas para as quais estão habilitadas, e por outro, deixando-as nessa situação o máximo tempo possível, ou que as circunstancias o permitam."*	**A.5.1** **A.5.4**
6	*"Desenvolver uma atividade profissional com um enorme potencial de crescimento e desenvolvimento."* *"Partilhar conhecimentos que são estado da arte com a comunidade nacional e NATO, o que releva a importância de estar presente em exercícios Ciber nacionais e NATO e executar ações Ciber que são incomuns, e nalguns casos, legalmente não são permitidas em mais nenhuma organização…"*	**A.5.5** **A.5.6**
7	*"Eu tenho TC a programar e eles não se importavam de ficar a programar a vida toda, não se importavam de ficar TC, desde que a remuneração fosse de alguma forma evoluindo e não ficassem estagnados a ganhar a vida toda como TC"* *"se eu conseguisse manter os RH que formamos e damos especialização, ficava satisfeito, só que não os conseguimos manter, estamos sempre com a corda na garganta "* *"Nós no Exército damos uma boa formação de base aos oficiais, pomo-los a trabalhar numa primeira fase na estrutura da rede […], a partir daí começamos a dar formação específica na área da CD para eles se tornarem especialistas em CD."*	**A.5.3** **A.5.4** **A.5.5** **A.5.6**

	"... a existências de carreiras alternativas, carreiras técnicas nas FFAA, não existem"	
8	*"... uma gestão de pessoal com critérios bem definidos e aceites pelo chefes de cada ramo e CEMGFA, nomeadamente os períodos de inamovibilidade de acordo com o investimento em formação e o desempenho de funções. Por outro lado os militares nomeados para estas áreas não deverão ser prejudicados na sua carreira militar "*	**A.5.1** **A.5.4**
9	*"Para promover uma maior retenção destes militares, poder-se-á regulamentar o pagamento de um subsídio específico que teria como contrapartida um número mínimo de anos de serviço na CD,"* *"... é igualmente importante que se promova a valorização da carreira nesta área, tornando-a atrativa e compensadora, designadamente pela visibilidade e recompensa do trabalho que é desenvolvido (que não é evidente, nem sequer dentro das Forças Armadas)."*	**A.5.3** **A.5.6**
10	*A medida mais eficaz para melhorar a retenção destes elementos passa por regular, através de normativo, essa retenção."*	**A.5.4**

Fonte: (Autor, 2018**)**