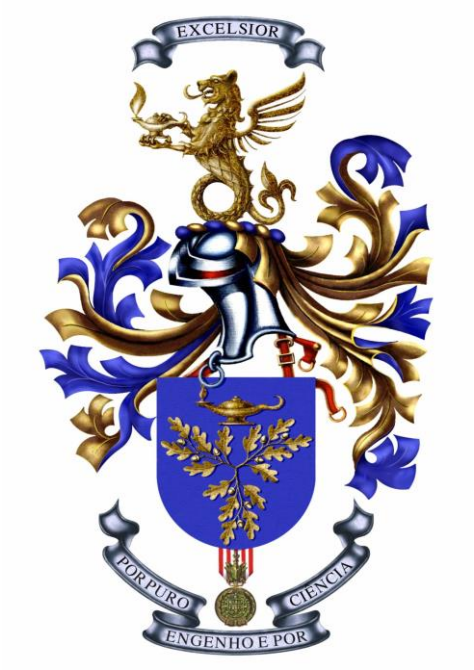
INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO DE ESTADO-MAIOR CONJUNTO
2019/2020



TII

LEVANTAMENTO DA ESTRUTURA ORGÂNICA DE GUERRA ELETRÓNICA E DE CIBERDEFESA PARA O NÍVEL TÁTICO NO EXÉRCITO PORTUGUÊS

João Daniel Gaioso Fernandes
MAJOR, TRANSMISSÕES

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

LEVANTAMENTO DA ESTRUTURA ORGÂNICA DE GUERRA ELETRÓNICA E DE CIBERDEFESA PARA O NÍVEL TÁTICO NO EXÉRCITO PORTUGUÊS

MAJOR, TRANSMISSÕES João Daniel Gaioso Fernandes

Trabalho de Investigação Individual do CEMC 2019/2020

Pedrouços 2020

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

LEVANTAMENTO DA ESTRUTURA ORGÂNICA DE GUERRA ELETRÓNICA E DE CIBERDEFESA PARA O NÍVEL TÁTICO NO EXÉRCITO PORTUGUÊS

MAJOR, TRANSMISSÕES João Daniel Gaioso Fernandes

Trabalho de Investigação Individual do CEMC 2019/2020

Orientador: TENENTE CORONEL, ARTILHARIA
João Ricardo de Sousa Barbosa e Dias da Costa

Pedrouços 2020

Declaração de compromisso Antiplágio

Eu, **João Daniel Gaioso Fernandes**, declaro por minha honra que o documento intitulado: **Levantamento da estrutura orgânica de Guerra Eletrónica e de Ciberdefesa para o nível tático no Exército Português**, corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Estado-Maior Conjunto 2019/2020** 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 **2020**

João Daniel Gaioso Fernandes

Agradecimentos

Ao TCor GNR Brito de Sousa que, como diretor do 3.º Curso de Planeamento de Operações no Ciberespaço, disponibilizou-se a desenvolver as diligências necessárias, que permitiram a minha participação em algumas das palestras realizadas no curso.

Aos militares do CCD do EMGFA, pela informação e tempo disponibilizado, dos quais saliento, o TCor Tm Jorge Vinagreiro e o 1Sar Tm Hugo Matos.

Aos militares da DCSI, que desenvolvendo trabalho na área da Ciberdefesa possibilitaram o acesso aos dados mais atuais dos projetos em curso, dos quais saliento, o TCor Tm David Antunes, Maj Tm Vítor Custódio e o Maj Tm Pedro Fernandes.

Na área de Guerra Eletrónica salientar a disponibilidade do Cap Tm Costa, comandante da Companhia de Guerra Eletrónica, que possibilitou a reunião de uma quantidade considerável de dados para a presente investigação, bem como transmitiu parte do seu vasto conhecimento e experiência na área.

Ao SCh Tm Vítor Esteves, pela amizade e disponibilidade em ajudar, não apenas nesta investigação, mas nos mais diversos trabalhos ao longo do CEMC.

Ao Maj Inf Dinis Faustino e ao Maj Art Diogo Serrão pela demonstração de amizade, que começou nos bancos da Academia Militar há mais de 20 anos.

Ao Maj Inf Borges, pela "co orientação" deste trabalho, demonstrando uma disponibilidade e paciência extremas, para corrigir e ajudar os amigos.

Ao meu Orientador, TCor Art Dias da Costa, pela sua exemplar postura e disponibilidade permanente, que mesmo em tempos de COVID em que assumiu novas funções em acumulação às já desempenhadas, sempre fez chegar orientações e contributos no sentido da melhoria deste trabalho.

Ao Diretor de Curso, CMG Carona Jimenez, pela paciência que teve para com os discentes do curso, nunca deixando de cumprir a sua tarefa em defesa destes.

Aos camaradas do CEM-C pelo caminho percorrido juntos, particularizando todos os residentes. Em especial ao Maj Inf Josias e ao Maj EngEl Zé Fernandes, pela amizade e pelas brincadeiras, que em muito ajudaram a ultrapassar esta etapa tão importante.

Por fim, às pessoas mais importantes na minha vida, os meus filhos e a minha esposa, pelo apoio incondicional e incentivo dado ao longo destes últimos meses, bem como pelo tempo que lhes privei da minha assistência.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Índice de Quadros

Resumo

O objetivo desta investigação é formular a estrutura de Guerra Eletrónica e de Ciberdefesa, para o Exército Português. Para o alcançar foi apresentada uma base concetual de referência, que além dos conceitos, identifica as estruturas da Organização do Tratado do Atlântico Norte e da União Europeia, ao que se seguiu a apresentação da mesma organização, referente a diversos países, a fim de estabelecer diferentes casos de estudo. Por fim foi apresentada a realidade nacional de Guerra Eletrónica e de Ciberdefesa. Para termo de comparação foram utilizados os vetores identificados para a edificação de uma capacidade militar.

Existe uma tendência de juntar as atividades ciber/eletromagnéticas, às Informações, num comando de componente, organizando desta forma, os comandos consoante os domínios operacionais. Na cimeira de Bruxelas em 2018, foi acordada a ativação do *Cyber Operations Centre*. Na sua dependência surgem as *Cyber Rapid Reaction Teams*, constituídas por um número reduzido de elementos, organizadas de um modo modular, disponíveis 24/7 e projetáveis.

A nível nacional, com o surgimento da ciberdefesa a arma de transmissões ganha uma nova importância e, por conseguinte, uma grande responsabilidade no campo de batalha, que terá de demonstrar estar à altura de o desempenhar.

Palavras-chave

Guerra Eletrónica, Ciberdefesa, *Cyber Operations Centre*, *Cyber Rapid Reaction Teams*

Abstract

The aim of this research is to formulate an Electronic Warfare and Cyber Defence framework for the Portuguese Army. To achieve this, a conceptual basis of reference was presented, which in addition to the concepts, identifies the structures of North Atlantic Treaty Organization and the European Union, followed by the presentation of the same organization, referring to several countries, in order to establish different case studies. Finally, the national reality of Electronic Warfare and Cyber Defence was presented. In order to compare, there were used the vectors identified for the formation of a military capability.

There is a tendency to combine cyber/electromagnetic activities with Intelligence, in a component command, thereby organizing commands depending on operational domains. At the Brussels summit in 2018, the activation of the Cyber Operations Centre was agreed. In its dependence arise the Cyber Rapid Reaction Teams, consisting of a small number of elements, organized in a modular way, available 24/7 and projectable.

At the national level, with the emergence of Cyber Defence, the Signals speciality benefits new importance, and therefore a great responsibility on the battlefield, which will have to demonstrate that it is up to the task of carrying it out.

Keywords

Electronic Warfare, Cyber Defense, Cyber Operations Centre, Cyber Rapid Reaction Teams

Lista de abreviaturas, siglas e acrónimos

A

AgrISTAR	Agrupamento *Intelligence, Surveillance, Target Acquisition & Reconnaissance*
AJP	*Allied Joint Publication*
APDSI	Associação para a Promoção e Desenvolvimento da Sociedade de Informação

B

BTm	Batalhão de Transmissões

C

C2	Comando e Controlo
CCD	Centro de Ciberdefesa
CCDE	Centro de Ciberdefesa do Exército
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CD	Ciberdefesa
CDCiber	Centro de Defesa Cibernética
CEMA	*Cyber Electromagnetic Activities*
CEME	Chefe de Estado-Maior do Exército
CFT	Comando das Forças Terrestres
CIRC	*Computer Incident Response Capability*
CNCS	Centro Nacional de Cibersegurança
CNO	*Computer Network Operations*
ComDCiber	Comando de Defesa Cibernético
CTGE	Centro de Treino de Guerra Eletrónica
COT	Centro de Operações Terrestres
CompGE	Companhia de Guerra Eletrónica
CPNI	*Centre for the Protection of National Infrastructures*

D

DCSI	Direção de Comunicações e Sistemas de Informação
DCOG	*Defence Cyber Operations Group*

Dep CD SegInfo	Departamento da Cibersegurança e Segurança da Informação
DoD	*Department of Defence*

E

ECOSF	Elementos da Componente Operacional do Sistema de Forças
EMGFA	Estado-Maior-General das Forças Armadas
ENSC	Estratégia Nacional de Segurança e Ciberdefesa
EU	*European Union*
EUA	Estados Unidos da América
EW	*Electronic Warfare*

F

FBI	*Federal Bureau of Investigation*

G

GE	Guerra Eletrónica

H

HUMINT	*Human Intelligence*

I

ISTAR	*Intelligence, Surveillance, Target Acquisition & Reconnaissance*

J

JADL	*Joint Advanced Distributed Learning*

N

NATO	*North Atlantic Treaty Organization*
NEDB	*NATO Emitter Database*
NEWAC	*NATO Electronic Warfare Advisory Committee*

O

OG	Objetivo Geral

OE	Objetivo Específico
OTAN	Organização do Tratado do Atlântico Norte

P

PelGE	Pelotão de Guerra Eletrónica
PEMGFA	Publicação do Estado-Maior General das Forças Armadas
PLA	*People's Liberation Army*

Q

QC	Questão Central
QD	Questão Derivada
QO	Quadro Orgânico

R

RTm	Regimento de Transmissões

S

SHAPE	*Supreme Headquarters Allied Powers Europe*
SegInfo	Segurança da Informação
SIGINT	*Signal Intelligence*
SIPRI	*Stockholm International Peace Research Institute*
SOF	*Special Operations Forces*
SOP	*Standard Operational Procedures*
SSF	*Strategic Support Forces*

T

TCOR	Tenente-Coronel
TIC	Tecnologias de Informação e Comunicação
TII	Trabalho de Investigação Individual
TTP	*Technical, Tactical and Procedures*

U

UE	União Europeia

1. Introdução

O que sabemos é uma gota, o que não sabemos é um oceano

Isaac Newton (1643-1727)

1.1. Enquadramento e justificação do tema

O presente estudo tem como tema "Levantamento da estrutura orgânica de Guerra Eletrónica e de Ciberdefesa para o nível tático no Exército Português". Após identificadas as estruturas correspondentes à Guerra Eletrónica (GE) e as atividades de Ciberdefesa (CD) existentes no Exército, bem como a sua adequabilidade, face aos desafios emergentes, existe necessidade de avaliar a sua sincronização no moderno campo de batalha.

Numa lógica de *Competitive Intelligence*, como sendo o "[…] processo sistemático e ético, de reunião, análise e gestão da informação, que pode afetar o planeamento, as decisões e as operações de uma organização […]" (Taborda & Ferreira, 2002, p. 61), associada à Guerra da Informação, que segundo Nunes, compreende a "[…] utilização da informação (recursos) e das tecnologias que a manipulam (vetores) como ferramentas (armas) contra eventuais adversários […]" (Nunes, 2015, p. 53), podemos depreender que quem obtiver a superioridade no domínio da informação, seja qual for o vetor utilizado, obterá vantagem sobre o adversário.

"A inclusão do domínio do ciberespaço na arte da guerra, vem sendo amplamente discutida nas áreas de Ciências e Tecnologia, Defesa, Estratégia e Relações Internacionais." (Sá, Machado, & Almeida, 2019, p. 90). Se compararmos a Guerra Cibernética com a Guerra Cinética, considerada por estrategistas ao longo dos tempos, desde Sun Tzu, Maquiavel, Carl von Clausewitz, Jomini, Liddell Hart, entre outros, ambas possuem um objetivo comum a alcançar: criar determinados efeitos no mundo real. Por outras palavras, a Guerra Cibernética só se justifica, se o esforço dos «soldados[1]» no combate, resultar, direta ou indiretamente, num efeito no mundo físico (Sá, Machado, & Almeida, 2019).

A GE utiliza energia eletromagnética, dirigida a sistemas inimigos que utilizem o espectro eletromagnético, no sentido de o controlar ou atacar. A ideia de ataque ciber eletrónico, que corresponde à sincronização de ataques no domínio cibernético em coordenação com a GE, corresponde a uma nova e aprimorada forma do desenvolvimento de ataques eletrónicos. Indo mais longe, ao explicar que um potencial alvo pode ser atacado

[1] Nesta situação, soldados cibernéticos.

por um sinal que atravessa o espectro eletromagnético com a finalidade de explorar uma porta de entrada num sistema informático, para posteriormente utilizar o fluxo de dados pela via cibernética (Yasar, Yasar, & Topcu, 2012). Sendo assim identificas as Atividades Ciber/eletromagnéticas (CEMA[2]), conceito desenvolvido no presente estudo.

Em 2008, na Geórgia, a Rússia antecedeu a ofensiva das suas forças convencionais, com ciberataques às infraestruturas críticas do Estado, a fim de desarticular alguns meios preponderantes para a resposta pronta da parte da Geórgia. Os referidos efeitos, podem ir desde a destruição física de estruturas do inimigo, à manipulação da informação por ele gerada. Já na Ucrânia, a Federação Russa desenvolveu operações de GE em coordenação com ciberataques, durante a anexação da Crimeia. São apenas dois exemplos recentes da importância que estes tipos de atividades têm nos conflitos modernos, que aumentam o potencial de combate de uma força, quando utilizadas de um modo coordenado e complementar. Foram apresentados no anexo A, alguns exemplos de atos de guerra no domínio do ciberespaço (Sá, Machado, & Almeida, 2019). A figura 1 demonstra a preparação de meios de GE russos, em apoio a operações militares na Ucrânia.

Figura 1 – Instalação de meios de GE russos

Fonte: Disponível em InformNapalm (2020)

[2] Utilizada a abreviatura do termo em inglês de *Cyber Electromagnetic Activities* (CEMA).

Considerando o apresentado anteriormente torna-se assim imperativo atentar à necessidade de edificar, ou desenvolver as capacidades que permitam a salvaguarda das nossas informações. Este desenvolvimento tem, de ter em consideração constantemente, o acompanhamento de toda a evolução tecnológica.

Nesta investigação em particular, interessa observar a vertente militar, que necessita de possuir estruturas sincronizadas transversal a todos os níveis, para que seja maximizada toda a componente de GE e de CD, fazendo face às ameaças cada vez mais evoluídas e potencialmente mais destrutivas.

> […] a humanidade não experimentou a guerra cibernética de forma tão ampla quanto o fez com a guerra cinética. Se, por um lado, os conhecimentos sobre a guerra cinética foram construídos com base em observações e registos feitos ao longo de milhares de anos, por outro, os conceitos sobre a guerra cibernética se baseiam em experiências adquiridas ao longo de algumas décadas. Ainda assim, os ataques cibernéticos já ocorridos representam uma valiosa fonte de informações para o estudo da guerra cibernética. (Sá, Machado, & Almeida, 2019, p. 93)

1.2. Objeto do estudo e sua delimitação

O objeto de estudo da presente investigação é a GE e a CD no Exército Português. A delimitação do estudo foi estipulada: (i) no tempo, baseada na evolução das orientações advindas dos acordos acertados na cimeira de Lisboa, em 2010; e (ii) no espaço, informação disponível no ciberespaço, ou seja, na *world wide web*, acessível a todos os seus utilizadores, sem a utilização de meios fraudulentos.

1.3. Objetivos da investigação

O objetivo geral (OG) desta investigação é: *Formular a estrutura orgânica de GE e de CD, para o Exército Português*. Para tal, a referida estrutura deverá ter a capacidade de coordenar e sincronizar as atividades de GE com as de CD, bem como identificar as possíveis melhorias, a realizar às atuais estruturas, a fim de permitir uma melhor inclusão destas áreas, no desenvolvimento e condução de operações militares.

De modo a alcançar o OG da investigação, é necessário atingir os objetivos específicos (OE), apresentados na tabela 1.

Tabela 1 – Objetivos específicos

OE	Descrição
1	Analisar as estruturas de GE e de CD da OTAN e da UE.
2	Analisar as estruturas de GE e de CD de países identificados como casos de estudo.
3	Analisar as estruturas de GE e de CD nacionais.

1.4. Questões da investigação

Decorrente do OG, é identificada a questão central (QC) desta investigação: *Que tipo de estrutura de GE e de CD, para o Exército Português, melhor se integra no seio das alianças a que Portugal pertence?*

Deduzindo dos OE, e considerando a QC, foram identificadas as seguintes questões derivadas (QD), apresentadas na tabela 2.

Tabela 2 – Questões derivadas

QD	Descrição
1	Quais as estruturas de GE e de CD da OTAN e da UE?
2	Como se caraterizam as estruturas de GE e de CD dos países identificados para os casos de estudo?
3	Quais as estruturas de GE e de CD nacionais?

1.5. Organização do estudo

O presente estudo encontra-se organizado do seguinte modo: (i) o segundo capítulo apresenta o modelo de análise, a metodologia de investigação utilizada e um enquadramento concetual, onde são apresentados os conceitos considerados mais pertinentes, a fim de estabelecer uma base de referência, para um entendimento comum; (ii) o terceiro capítulo, que cumpre o OE1 e responde à QD1, explora as estruturas e estratégias da OTAN e da UE; (iii) o quarto capítulo que, cumpre o OE2 e responde à QD2, apresentada as estruturas de países identificados como possíveis casos de estudo; (iv) num quinto capítulo que, cumpre o OE3 e responde à QD3, apresentada as estruturas nacionais de GE e CD; e (v) no sexto capítulo é apresentada a comparação dos resultados obtidos.

A figura 2 apresenta uma descrição, por intermédio de um esquema, do modelo de análise utilizado no desenvolvimento do presente estudo.

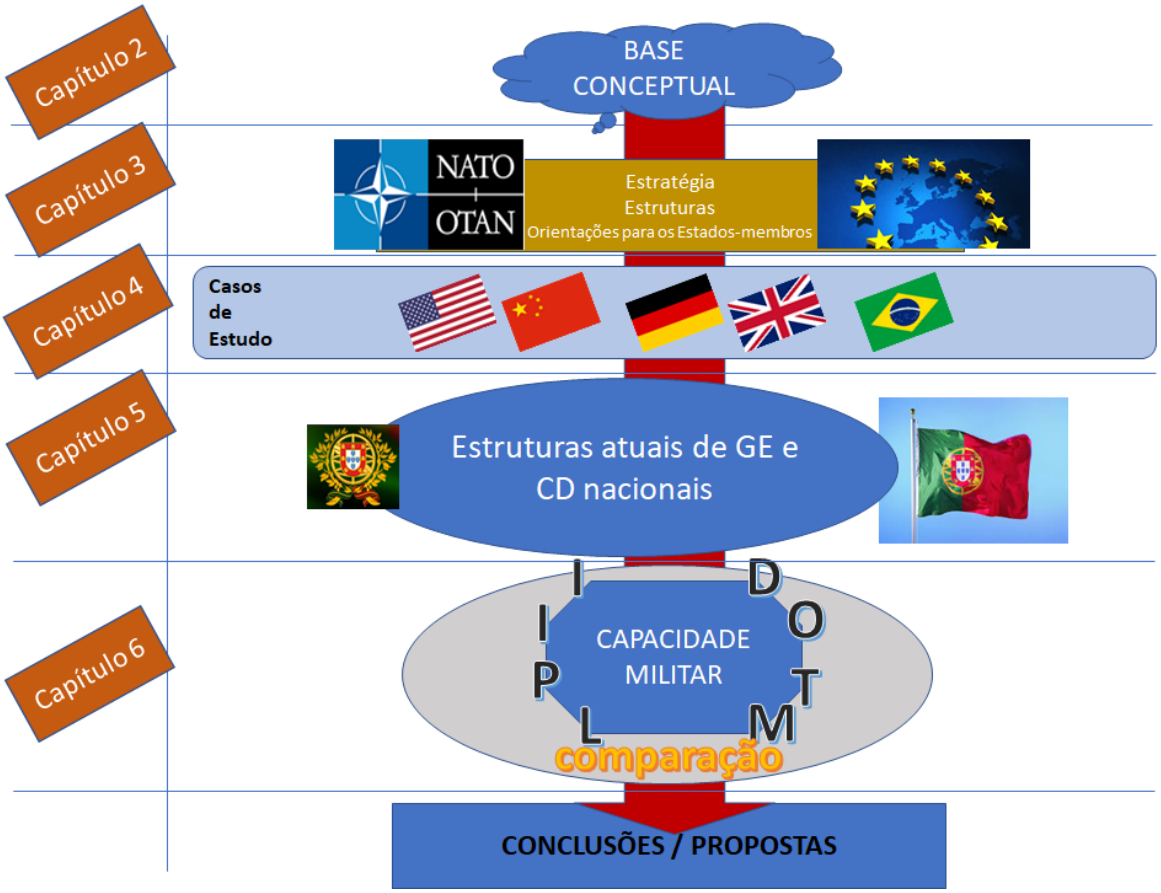


Figura 2 – Organização da investigação – modelo representativo

2. Opções metodológicas e método de investigação

O presente capítulo apresenta o modelo de análise utilizado no estudo, tendo em consideração os conceitos estruturantes, associados às respetivas dimensões e comparados, tendo por base os vetores elencados para a edificação de uma capacidade militar. Na parte destinada à metodologia de investigação definida, é apresentado o percurso, estratégia de investigação e desenho de pesquisa, que permite alcançar os resultados obtidos.

2.1. Modelo de análise

A fim de apresentar o modelo de análise a utilizar, existe, nesta fase, a necessidade de apresentar as variáveis que nos vão auxiliar a comparar os resultados, que se encontram correlacionadas com conceito de capacidade militar. Este pode ser definido, de acordo com o AAP-06 da OTAN (2018, p. 23), como a criação de um efeito, através de um conjunto integrado de aspetos categorizados pelos seguintes vetores[3]: (i) Doutrina; (ii) Organização; (iii) Treino; (iv) Material; (v) Liderança; (vi) Pessoal; (vii) Infraestruturas; e (viii) Interoperabilidade.

O quadro 1 apresenta o modelo de análise de investigação utilizado.

Quadro 1 – Modelo de Análise

Conceitos estruturantes	Dimensões	Variáveis
Guerra Eletrónica e *Ciberdefesa*	Estruturas OTAN e UE.	Doutrina Organização Treino Material Liderança Pessoal Infraestruturas Interoperabilidade
	Estruturas de países identificados para os casos de estudo.	
	Estruturas nacionais.	

2.2. Metodologia de investigação

No decorrer deste estudo seguiu-se um raciocínio indutivo, na medida em que, é considerada a estratégia das alianças, apresentadas estruturas de países identificados para casos de estudo, bem como a estrutura nacional, tendo sido realizada a respetiva comparação com base nos vetores de edificação de uma capacidade militar. O desenho de pesquisa utilizado foi o caso de estudo, numa ótica de *bench leaning*.

[3] Dimensões conhecidas pela sigla DOTMLPF-I (iniciais em inglês) nos conceitos da OTAN.

Na fase exploratória, foi tida em consideração a construção de um quadro de referência que considerou as visões estratégicas das organizações às quais Portugal pertence. Foram conduzidas entrevistas exploratórias e diversos contatos com as entidades de relevância, associadas ao objeto de estudo.

Na fase analítica, foi consolidado o processo de revisão da literatura, o autor deste estudo acompanhou o 3.º Curso de Planeamento de Operações no Ciberespaço, que se realizou no IUM e participou na conferência, concretizada pelo Estado-Maior General das Forças Armadas (EMGFA) em 16 de janeiro de 2020, no IUM e intitulada *A Ciberguerra: como travar e vencer num conflito global*. Ainda nesta fase, existiu a necessidade de desenvolver mais entrevistas semiestruturadas, a fim de complementar a investigação.

Por fim, na fase conclusiva, almejou-se atingir as conclusões, corolário do estudo, considerando por base todas as informações recolhidas da documentação consultada, relacionando com a experiência e os *inputs* obtidos das entrevistas desenvolvidas.

2.2.1. Participantes e procedimentos

Os organismos participantes na presente investigação, que disponibilizaram dados para análise, foram o Centro de Ciberdefesa (CCD) do EMGFA, o Estado-Maior do Exército (EME), pela Divisão de Doutrina, Normalização e Lições Aprendidas, a Direção de Comunicações e Sistemas de Informação (DCSI) e o Regimento de Transmissões (RTm). Em termos internacionais, foram desenvolvidos contatos no *North Atlantic Treaty Organization* (*NATO*) *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), bem como, com outros militares que desempenharam funções ligadas à CD e à GE, tanto na OTAN como na União Europeia (UE).

2.2.2. Instrumentos de recolha de dados

Dentro dos organismos anteriormente mencionados, foram desenvolvidas entrevistas exploratórias e semiestruturadas, quando identificada a necessidade, a determinados indivíduos. Também de salientar que muitos deles, foram palestrantes em seminários ou/e cursos assistidos pelo autor.

2.2.3. Técnicas de tratamento de dados

O quadro 2 apresenta os pontos de contacto dos organismos, bem como palestrantes, dos quais foram recolhidos dados apresentados no presente estudo.

Quadro 2 – Análise do processamento dos dados recolhido

Entrevistados	**Seminários** e **Cursos**	**QD1**	**QD2**	**QD3**
TCor Tm Correia (CTGE) TCor Tm Lopes (BrigMec) Cap Tm Costa (CompGE)				GE nacional
TCor Tm Vinagreiro (CCD) TCor Tm Antunes (DCSI) Maj Tm Custódio (DCSI) Maj Tm Fernandes (DCSI)	• "*A Ciberguerra: como travar e vencer num conflito global*" • "*3.º Curso de Planeamento de Operações de Ciberdefesa*" • *ADL 076 Cyber Defence Awareness*			CD nacional
CMG Fialho Jesus (CCD) TCor Tm Vinagreiro (CCD) Maj Tm Susana Pinto (EME)		CD *NATO*		
TCor Tm Carvalho (MDN) TCor Tm Teixeira (CCDCOE)		CD e GE da UE		
Maj Tm Susana Pinto (EME) Cap Tm Costa (CompGE)		GE *NATO*		
TCor Tm Vinagreiro (CCD) Cap Tm Costa (CompGE)			EUA Alemanha Reino Unido Espanha França China Brasil Rússia	
TCor EXE BRA Vinícius Vasquez (CDCiber)			Brasil	

2.3. Quadro teórico de referência

Nos dias de hoje, é bastante comum a utilização do termo ciberespaço, apesar de ser um termo, que de acordo com a Associação para a Promoção e Desenvolvimento da Sociedade de Informação (APDSI), surgiu em 1984 por William Gibson, no seu romance *Neuromancer*, quando refere "*A year here and he still dreamed of cyberspace* […]" (Gibson, 1984, p. 3), definindo-o como "[…] *a graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity* […]" (Gibson, 1984, p. 48).

O Centro Nacional de Cibersegurança (CNCS) define nos seus conceitos, ciberespaço como sendo uma "[…] metáfora usada para descrever o espaço não físico criado por redes de computadores, nomeadamente pela Internet, onde as pessoas podem comunicar de diferentes maneiras […]" (APDSI, 2020 cit. por CNCS, 2020).

De acordo com a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023 (ENSC, 2019), o "Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.". O mesmo documento define também o conceito de Cibersegurança, que se entende pertinente de identificar.

> […] Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem. (ENSC, 2019)

A política da OTAN estabelece como conceito de GE, associado a uma ação militar que explora a energia eletromagnética, tanto de modo passivo como ativo, a fim de determinar a *situational awareness* e criar efeitos no inimigo (NATO, 2012, pp. 1-1). Esta definição é consensual entre os estados-membros no seio da aliança, com Portugal a não ser exceção.

De modo a definir o meio utilizado pela GE, o autor recorreu ao dicionário de português online Priberam, que no âmbito da física, define espectro, como o "[…] registo de dispersão ou distribuição de energia ou radiação." e eletromagnético, relacionado com eletromagnetismo, que é a "[…] ciência que trata das relações existentes entre a eletricidade e o magnetismo […]" (Priberam, 2020). Relacionando as duas definições, podemos inferir de que o espectro eletromagnético é uma gama de ondas eletromagnéticas, que permite o movimento de energia. Esta energia, por sua vez, permite que seja inserida informação, descodificada por determinados sistemas, como são exemplos os rádios de comunicações e os radares.

De acordo com a figura 3, é possível identificar o modo como o espetro eletromagnético e o ciberespaço são transversais aos restantes domínios operacionais, devendo ser tidos em consideração, para a condução de operações militares.

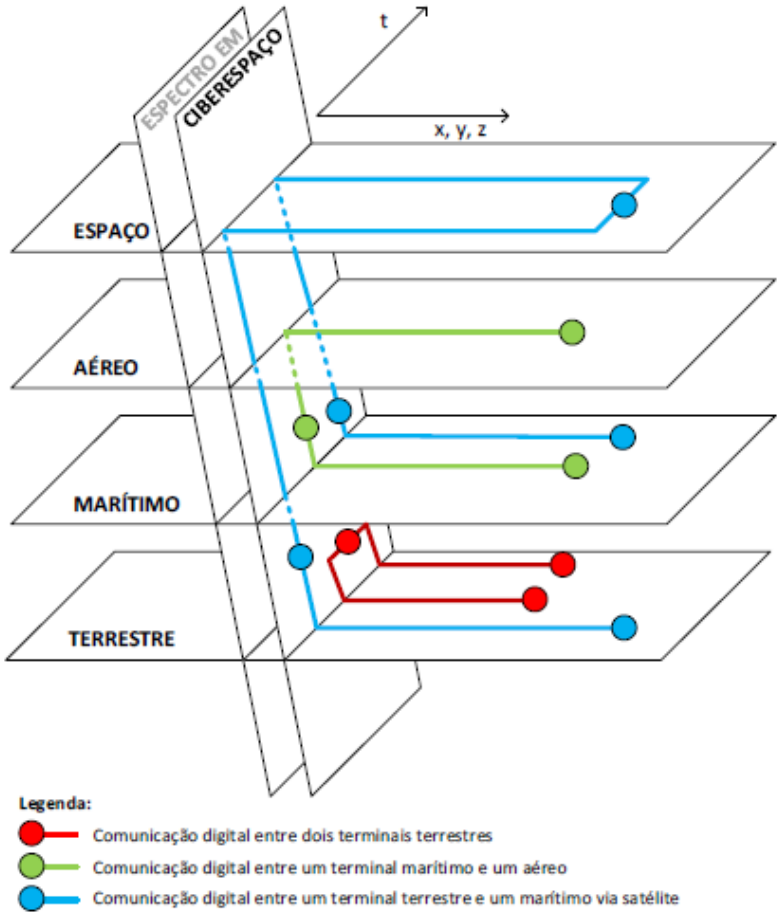


Figura 3 – Os 5 Domínios Operacionais[4]

Fonte: Honorato, Santos, & Mateus (2017)

O *Allied Joint Publication* (AJP) – 3.6 – *Allied Joint Doctrine for Electronic Warfare* disponibiliza um conjunto de conceitos ao nível operacional, a fim de, habilitar os comandantes a desenvolver o planeamento, a coordenar e monitorizar as atividades de GE.

A nível de CD o AJP – 3.20 – *Cyberspace Operations Doctrine*, produzido em 2016, como *draft* e entregue aos estados-membros para dar a possibilidade de sugerirem alterações, foi aprovado no início do ano de 2020. Esta publicação demonstra o esforço da OTAN em construir o edifício doutrinário da aliança, no sentido de permitir também aos seus estados-membros a sua definição doutrinária coerente.

Em 2016, através da publicação *Capability Codes and Capability Statements*, a OTAN identifica como foco primário a necessidade de efetuar o desenvolvimento de várias capacidades militares por parte dos estados, entre as quais a Ciberdefesa (NATO, 2016). Neste documento é apresentado o conceito de uma unidade de CD projetável, designada por

[4] Apenas em 2019 a OTAN reconhece o espaço como novo domínio de operações (NATO, 2019).

(CD-DEPLOY), dimensionada para o apoio a uma brigada, onde surgem particularizados os requisitos necessários para o estabelecimento desta unidade, apresentada a sua descrição no quadro 4 no anexo B. A nível nacional, está a decorrer um projeto no Exército, dando cumprimento à Lei de Programação Militar, que contempla o respetivo financiamento, para edificação desta capacidade.

A UE, através do *Operational Guidance for the European Union's* (EU) *international cooperation on cyber capacity building* (EU, 2018), identifica o modo como os estados-membros devem edificar a capacidade de CD, tendo também por base a *Cybersecurity Strategy* (EU, 2013), identificada desde junho de 2013.

A doutrina OTAN, bem como as dos países aliados, enquadra as atividades conduzidas no ciberespaço e as atividades conduzidas no espetro eletromagnético com interdependentes, existindo algumas áreas de sobreposição. Atualmente, o Exército Português possui no seu Sistema de Forças duas unidades com valências nas áreas referidas: a Companhia de GE[5] (CompGE) e o Módulo Tático *Computer Incident Response Capability* (CIRC[6]) (ModTat CIRC).

> […] surge, interceção entre ações cibernéticas e a guerra eletrónica "convencional". Ambas partem dos mesmos fundamentos estratégicos (roubar informações, enganar e inviabilizar a ação do inimigo) de tal forma, que já podemos falar de um espaço de conflito "ciber-eletrónico", que envolve a utilização de tecnologia de guerra eletrónica e diversos tipos de *malware* utilizando a tecnologia *wifi* como modo de transmissão. (Neto, 2017, p. 201)

Na Publicação de Operações do Exército, as atividades Ciber/eletromagnéticas encontram-se divididas segundo duas linhas de esforço: (i) operações no ciberespaço; e (ii) a GE, conforme figura 4.

[5] Quadro Orgânico (QO) (09.02.08) de 13mai15.
[6] QO (09.03.02) de 15fev16.

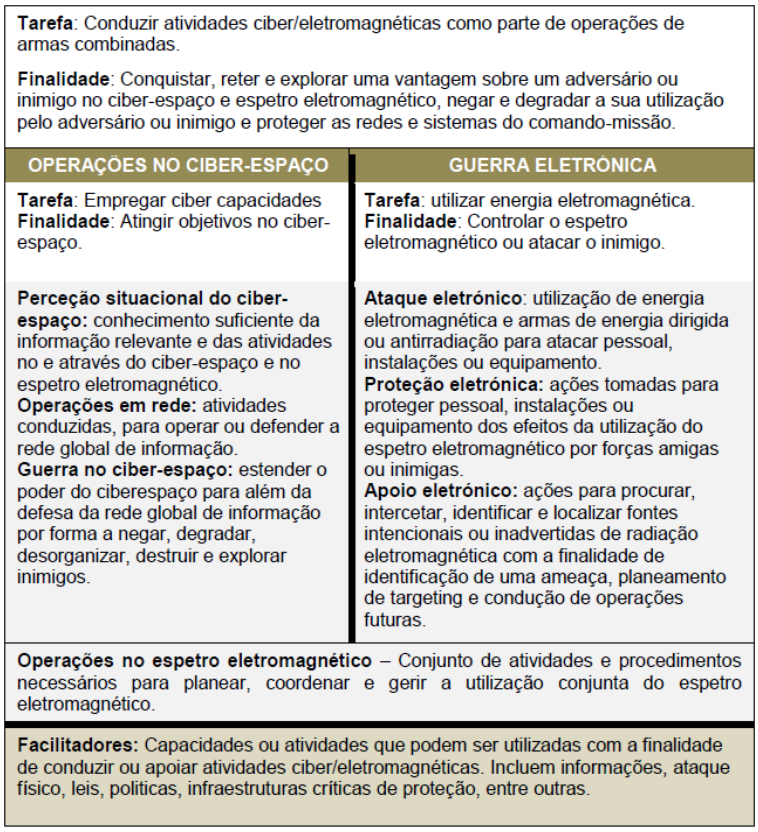


Figura 4 – Linhas de esforço das atividades ciber/eletromagnéticas

Fonte: PDE 3-00 Operações, Exército Português (2012, pp. 4-16)

Uma breve análise à figura anterior, permite inferir que as linhas de esforço possuem um *modus operandi* semelhante, sendo possível efetuar-se uma separação em três conjuntos de ações: (i) as de pesquisa, desenvolvidas normalmente durante o pré conflito; (ii) as defensivas, aquando da identificação de um possível ou já efetivado ataque; e por último (iii) as ações de ataque, que se regem por normas e legislação bastante rígidas. No apêndice A são apresentados outros conceitos, de modo a complementar o quadro teórico apresentado.

3. As estruturas de Guerra Eletrónica e de Ciberdefesa na OTAN e UE

O presente capítulo destina-se a abordar as estratégias e estruturas da OTAN, aliança de índole militar, bem como o equivalente à UE, aliança de âmbito predominantemente económico. Desde modo podemos identificar e, caso necessário corrigir, possíveis desalinhamentos que Portugal possa ter para com as suas alianças de referência.

De acordo com o *Heads of State and Government* na cimeira de Bruxelas, "As capacidades desenvolvidas pelas iniciativas de defesa da UE e da OTAN, devem ser coerentes, complementares e interoperáveis. Devem estar disponíveis para ambas as alianças, sujeitas às decisões soberanas dos seus estados-membros […]". Também nesse sentido, *Jens Stoltenberg*, secretário-geral da OTAN, salienta que "Vamos assegurar que as estratégias de desenvolvimento […] são complementares, a fim de ser possível trabalhar juntos de modo rápido e eficaz, em caso de efetivação de uma ameaça híbrida contra qualquer um dos nossos estados-membros […]" (NATO, 2018, p. 21).

A cooperação OTAN-UE tem vindo a ser patenteada também nas questões relacionadas com o ciberespaço, obrigando a que os estados-membros se comprometam a reforçar as suas capacidades nesta área, nomeadamente no investimento em áreas como a formação e educação. Ambas as alianças cooperam por intermédio de um acordo de cooperação técnica e de CD, tendo Portugal defendido a Academia *NATO*, em Oeiras, como um modo de reforçar a referida cooperação, assegurando uma política de não duplicação de meios e de complementaridade.

3.1. Organização do Tratado do Atlântico Norte

O *NATO Electronic Warfare Advisory Committee* (NEWAC), é o organismo responsável pelo desenvolvimento da política, doutrina e conceitos de Comando e Controlo (C2) da OTAN, bem como pela monitorização e apoio às operações desenvolvidas pela aliança no âmbito da GE. O comité é composto por representantes de todos os países OTAN ao nível do Comando Estratégico (NATO, 2011).

É entendimento da OTAN, demonstrado ao longo dos últimos cerca de 70 anos, a importância da GE, como ação militar que explora o espectro eletromagnético a fim de garantir uma superioridade informacional, através de uma *situational awareness*, com a finalidade de abranger efeitos quer ofensivos, quer defensivos. Desde ataques a sistemas de radar, até ao empastelamento das comunicações, pode ser utilizada nos domínios de operações na terra, ar, mar ou espaço, a fim de apoiar o ciclo das informações. A rápida

evolução tecnológica, coloca um grande desafio à aliança, no sentido da permanente atualização dos meios (NATO, 2019).

O NEWAC, na sua reunião do passado mês de novembro (NATO, 2019), salienta que a implementação de uma estratégia irá exigir a capacidade de treinar com pessoal experiente, a disciplina de GE. A política da OTAN nesta área é bastante influenciada pelas capacidades que as nações possuem, bem como as lições aprendidas dos exercícios nacionais, bilaterais ou multinacionais e exercícios ao nível operacional (Kabasakal, 2019).

O *Joint Electronic Warfare Core Staff*, na dependência direta do *Supreme Headquarters Allied Powers Europe* (SHAPE), é responsável pelo planeamento, integração e condução do desenvolvimento das operações de GE. O *NATO Emitter Data Base Advisory Group*, o organismo responsável pela *NATO Emitter Database* (NEDB), que tem como objetivo a partilha da *Common Electronic Warfare Order of Battle*. O *NATO Electronic Warfare Working Group*, é implementado quando identificada a sua necessidade, para a elaboração de trabalhos de GE. Atualmente encontra-se dedicado à atualização da NEDB.

O exercício *Naval Electro Magnetic Operations* (NEMO), realizado entre 31 de outubro e 05 de novembro de 2019, ao largo da costa do Reino Unido, teve a participação de 13 países membros da OTAN, tendo tido particular incidência na simulação de defesas navais antiaéreas, de modo a verificar o estado da arte das defesas eletrónicas contra a ameaça dos misseis hipersónicos (NATO, 2019).

As cimeiras de 2014 e 2016 foram as que mais relevância deram ao conceito de CD na OTAN, pois identificaram, que as ameaças à segurança da aliança neste domínio, começavam a tornar-se mais frequentes, complexas, com uma capacidade destrutiva ou coerciva potencialmente mais elevadas. O ponto 20 da declaração da *Brussels Summit* (NATO, 2018, p. 7), aborda a questão de como a aliança do Atlântico encara e pretende abordar a questão da CD. Para uma organização de âmbito militar com índole, particularmente defensivo, desenvolve capacidades que se enquadram em "[…] *to defend each other* […]", no desenvolvimento de operações em todos os seus domínios, o que inclui, desde 2016 o domínio do ciberespaço.

Na cimeira de Bruxelas em 2018, os países aliados, concordaram com a ativação do *Cyberspace Operations Centre* (CyOC), na Bélgica, fortalecendo deste modo a estrutura de comando da OTAN, garantindo uma *situational awareness* atualizada, bem como, estabelecendo a coordenação operacional de todas as atividades neste domínio. Em fevereiro de 2019, são enviadas linhas orientadores para os estados-membros, identificando um vasto

número de ferramentas, a fim de que estes próprios tenham a capacidade de fortalecer as suas redes, e ao mesmo tempo criar um conjunto de organismos interoperáveis, com a capacidade de coordenar ações entre si.

O principal foco da OTAN é proteger as próprias redes, presentes no ciberespaço, incluindo as de operações, de modo a demonstrar a sua resiliência por toda a aliança. Para tal, mantém em *standby* as *NATO Cyber Rapid Reaction Teams,* que se focam nas ameaças e incidentes detetados nas próprias redes, podendo, em caso de solicitação, auxiliar os estados-membros. As responsabilidades destas equipas são: (i) proteger as próprias redes; (ii) operar ciberespaço em operações; e (iii) auxiliar o aumento na ciber resiliência nos países da organização. São constituídas por um número reduzido de elementos, organizadas de um modo modular, disponíveis 24/7 e, em caso de necessidade, prontas a ser projetadas.

O *Cyber Coalition*, é o exercício militar no domínio do ciberespaço, que reúne mais participantes em todo o mundo, e que tem como objetivos principais, testar a capacidade de defesa da OTAN, bem como a de outras redes nacionais, a fim de garantir uma segurança coletiva e demonstrar a unidade transatlântica (NATO, 2019).

Uma das grandes preocupações é o cumprimento do direito internacional, tendo para tal como publicação de referência o *Manual de Tallin* 2.0, publicado em 2017. Este tem a finalidade de reunir aspetos legais, técnicos, estratégicos e avaliações operacionais de vários cenários, a serem usados como modelo para os Comandos Ciber (CCDCOE, 2017). Esta publicação constitui-se como uma referência, que contém linhas orientadoras, não possuindo carater vinculativo ao direito internacional.

No que concerne a projetos, após a identificação das orientações políticas, Portugal desenvolveu diligências no sentido de participar em projetos neste domínio, dos quais se destaca, o projeto *Smart Defence*, *Cyber Defence Education and Training*[7], no âmbito da OTAN, que o país liderou de 2014 a 2019.

3.2. União Europeia

Em conjunto, a OTAN e a UE, cooperam por intermédio de um *Technical Arrangement* na área de CD, que foi assinado em fevereiro de 2016. Esta cooperação tem como principal objetivo enfrentar os desafios comuns, com que se deparam ambas as alianças, e potenciar a edificação de capacidades, nomeadamente nas áreas de troca de informação, treino, pesquisa e exercícios (NATO, 2020).

[7] Este projeto teve como principal objetivo o desenvolvimento de plataformas ligadas à formação e treino.

Existem diversas áreas possíveis de cooperação UE-OTAN, das quais se salienta a condução de exercícios e a partilha das lições aprendidas. Este desenvolvimento, deve ser ajustado através dos conhecimentos aprendidos e partilhados entre todos os participantes nos mais diversos exercícios ciber de cooperação entre os estados-membros, dos quais saliento, PACE, CYBRID e Cyber Europe, da responsabilidade da UE e o Cyber Coalition e CMX da responsabilidade da OTAN (Vass, 2019).

O seu nível de ambição é incentivar a edificação e desenvolvimento de capacidades dos estados-membros, no sentido de fortalecer a parceria em diversas áreas, como é o caso das comunicações e da cibersegurança (Council of the European Union, 2016).

Existem alguns projetos no âmbito da GE que interessa salientar, a decorrer no âmbito da *Permanente Structured Cooperation* (PESCO): (i) o *Airborne Electronic Attack*; (ii) o *EW Capability and Interoperability for future Joint Intelligence and Reconnaissance* (JISR) *Cooperation*; e (iii) o *Joint* European Union Intelligence School (JEIS).

A figura 5 apresenta um folheto referente a uma conferência, realizada na Academia Militar, na Amadora, referente à cooperação OTAN-UE nos projetos de *Smart Defence*.

Figura 5 – Cooperação OTAN-UE - *Smart Defence Projects*

Fonte: Academia Militar (2019)

3.3. Síntese conclusiva

Podemos identificar que a OTAN, apesar de apenas em 2016 ter reconhecido o ciberespaço como domínio de operações, atribuiu relevância à CD principalmente desde a cimeira de 2014, com a definição da sua estratégia, bem como indicando ao estados-

membros as devidas orientações. Já a UE apresenta-se como um bom parceiro, principalmente nos aspetos de treino e formação, ficando deste modo concretizado o OE1 e respondida a QD1.

4. Identificação dos estudos de caso

Neste capítulo foi realizada uma análise a outros países, ao nível da CD e da GE. A escolha dos vários países analisados focou-se, nos que possuem uma estratégia mais completa e adequada à realidade da rápida evolução das ameaças. De salientar que, em particular a GE, por ser uma ação muito interligada com operações militares, é uma temática que ao longo dos tempos os países têm desenvolvido esforços no sentido de a manter em sigilo nacional, dificultando, deste modo a sua investigação, principalmente em plataformas *open source*, como é a *world wide web*.

4.1. Estados Unidos da América

O *United States Cyber Command* (USCYBERCOM) foi criado oficialmente a 23 de junho de 2009, na dependência do *US Strategic Command*. Em 18 de agosto de 2017, é elevado a um dos 11 *Unified Combatant Command*[8] (US DoD, 2017). Tem como missão "*[…] synchronize, and coordinate cyberspace planning and operations, to defend and advance national interests, in collaboration with domestic and international partners"* (USCYBERCOM, 2020). O seu foco principal centra-se em três áreas: (i) defender a intranet do *Department of Defence* (DoD); (ii) apoiar os comandantes das unidades operacionais e combatentes, na execução das suas missões em qualquer parte do mundo; e (iii) capacitar o país, fortalecendo-o para fazer face a todos os ciber ataques contra a nação (USCYBERCOM, 2020). A figura 6 apresenta os comandos ciber a nível de componente na dependência do USCYBERCOM.

Figura 6 – Organograma da estrutura Ciber das FFAA dos EUA

Fonte: Adaptado do website do *US Cyber Command* (2020)

[8] É um comando das FFAA composto pelo menos por unidades de dois ou mais ramos (US DoD, 2017).

O US *Army Cyber Command* (ARCYBER), constitui um comando de componente ao nível operacional, responsável pelas Operações no Ciberespaço, de acordo com as delegações atribuídas pelo USCYBERCOM. Desenvolve operações ofensivas, defensivas e Operações de Informação em Rede, em estreita coordenação e sob a orientações do USCYBERCOM (ARCYBER, 2020).

O ARCYBER tem na sua dependência quatro unidades, apresentadas no quadro 7 do apêndice B, desenvolvendo operações 24/7, com os seus cerca de 16500 militares e civis. Atualmente conduz operações contra ameaças como o ISIS, e outras ameaças no ambiente ciber, defende as redes militares, assegura o bom funcionamento de plataformas de armas, através de medidas ciber defensivas e protege infraestruturas críticas dos Estados Unidos da América (EUA) (ARCYBER, 2020).

A figura 7 apresenta um organograma que demonstra o modo como a doutrina dos EUA identifica as CEMA.

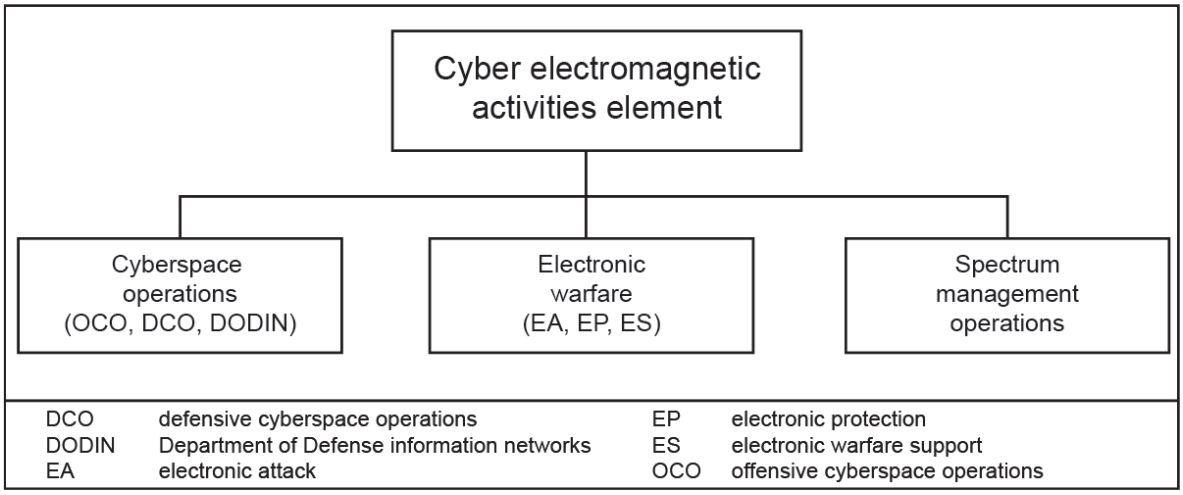


Figura 7 – Conceito de CEMA de acordo com doutrina dos EUA

Fonte: FM 3-38 CEMA (2014, pp. 2-2)

Ao nível tático de salientar desde 2015, no exército dos EUA, a implementação das CEMA *Teams*, passíveis de serem utilizadas em apoio a uma unidade escalão brigada (Signal, 2018).

4.2. China

Entender a estrutura, as estratégias e a organização ciber da China não é tarefa fácil, pois, não se encontra disponibilizada uma estratégia claramente definida associada aos respetivos objetivos e correspondente caminho para os alcançar. Envolto nesta cortina de mistério, e com uma maior necessidade de desenvolver operações no ciberespaço, foi criada

a Comissão Central de Segurança na Internet e Informação, com dependência direta do presidente Xi Jinping (Raud, 2016).

No que respeita aos conceitos, para os chineses é comum utilizar o termo de informação em substituição do termo ciber, como por exemplo o conceito de *information space*, equiparado a *cyberspace*, *information security* a *cybersecurity*, ou mesmo *information warfare* com correspondência a *cyber warfare* (Raud, 2016).

O conceito de informações apresenta-se como central no pensamento militar chinês, estando bastante interligado com o ciberespaço, o que leva a que a China demonstre uma clara ambição no sentido de adquirir a superioridade neste domínio (Lindsay, 2012).

O desenvolvimento da tecnologia chinesa é inquestionável, tendo mesmo o ocidente alegado que ferramentas dispersas pelo mundo alimentam o sistema de informações militar, e por consequência o regime, em prol de espionagem política ou económica, a fim de adquirir uma vantagem estratégica no contexto da geopolítica internacional. Assim, em 2015, o Departamento de Comunicações do Departamento do Estado-Maior é restruturado para Departamento de Informações, adicionando à estrutura de comunicações as pequenas células de informações que se encontravam dispersas (Thomas, 2012).

São criadas em 2014 as *Strategic Support Forces* (SSF), organismos que garantem, ao *People Liberation Army* (PLA), entre outras valências, a pesquisa e obtenção de informações de modo a alcançar a vantagem ambicionada, para a segurança nacional da China. Incluído nas SSF encontra-se o *Cyberspace Strategic Intelligence Centre* (Costello, 2016a).

A estrutura do SSF ainda é um assunto um pouco incerto, mas podemos concluir da pesquisa realiza que possui na sua dependência as áreas relacionadas com o espaço, o ciberespaço e a GE (Costello, 2016b).

De acordo com uma pesquisa realizada por Jeffrey Knowng existem outros grupos relevantes a atuar no ciberespaço, a partir da China, além das unidades afetas ao PLA. Os *Hacktivists* e as *Cyber Militias*, aparentemente atuam independentes do governo (Kwong, 2012). Os conceitos associados encontram-se apresentados no apêndice A.

4.3. Alemanha

As Operações no Ciberespaço e no domínio informacional, destinam-se a caraterizar o ambiente operacional, através dos aspetos de criação de efeitos militares no inimigo, segurança e proteção da força, informações, indicadores e avisos e garantir o cumprimento da lei. As responsabilidades encontram-se distribuídas pelo Ministério do Interior, que é responsável pela contra informação no domínio ciber, pelo Ministério dos Negócios

Estrangeiros, que é responsável pelos assuntos ciber relacionados com os negócios estrangeiros, bem como os assuntos que envolvam algum tipo de diplomacia, e por fim o Ministério da Defesa que garante toda a Ciberdefesa. Todos os esforços destas entidades combinados garantem a autonomia e proteção do estado, sob a égide do Comando do Espaço Cibernético e da Informação (Kdo CIR) (LTC Wolfram, 2019).

> […] a nova dimensão do espaço cibernético e da informação, com base nas suas oportunidades e riscos, é de grande importância para a política de segurança alemã. O "ramo" Ciber reúne capacidades militares que criam condições para uma Defesa mais eficaz nesta dimensão. A segurança no espaço cibernético e da informação é uma tarefa nacional […]. (COR Baltazar, 2019)

O Kdo CIR é um comando de componente, ao mesmo nível do Exército, da Força Aérea, da Armada, dos Serviços Médicos e do Apoio Conjunto Logístico, todos na dependência do Ministério da Defesa. Constitui-se como único responsável por garantir a superioridade nos domínios do Ciberespaço e das Informações.

A doutrina alemã acrescenta, ao domínio do ciberespaço, operações em dois outros domínios militares: (i) o ambiente eletromagnético; e (ii) o domínio militar informacional. Tudo em conjunto é designado o Espaço Informacional, sendo este espaço a área de operações do Kdo CIR. As capacidades CIR encontram-se divididas de acordo com o Quadro 8 em apêndice B.

Os serviços CIR encontram-se divididos por: (i) Centro de Situação, onde é caraterizada a *situational awareness* para a FFAA alemãs e para as instituições governamentais; (ii) o *Centro de Operações Ciber*, onde se encontram incluídas as *red teams*; (iii) o Centro de Desenvolvimento de *Software*; (iv) o Centro de Segurança CIR; e (v) o Reconhecimento e Operações.

De salientar da figura 8, o Reconhecimento e Efeitos numa unidade escalão Regimento, onde se inclui equipas de GE e de Informações, por outro lado uma segunda unidade escalão Regimento, onde se incluem os serviços IT. Por último, uma unidade escalão brigada para a informação Geográfica. No que respeito a pessoal, possui um conjunto de cerca de 14000 pessoas[9], prevendo-se cerca de 15000 aquando da sua FOC, prevista para 2021 (COR Baltazar, 2018).

[9] 2500/7400/2400/1700.

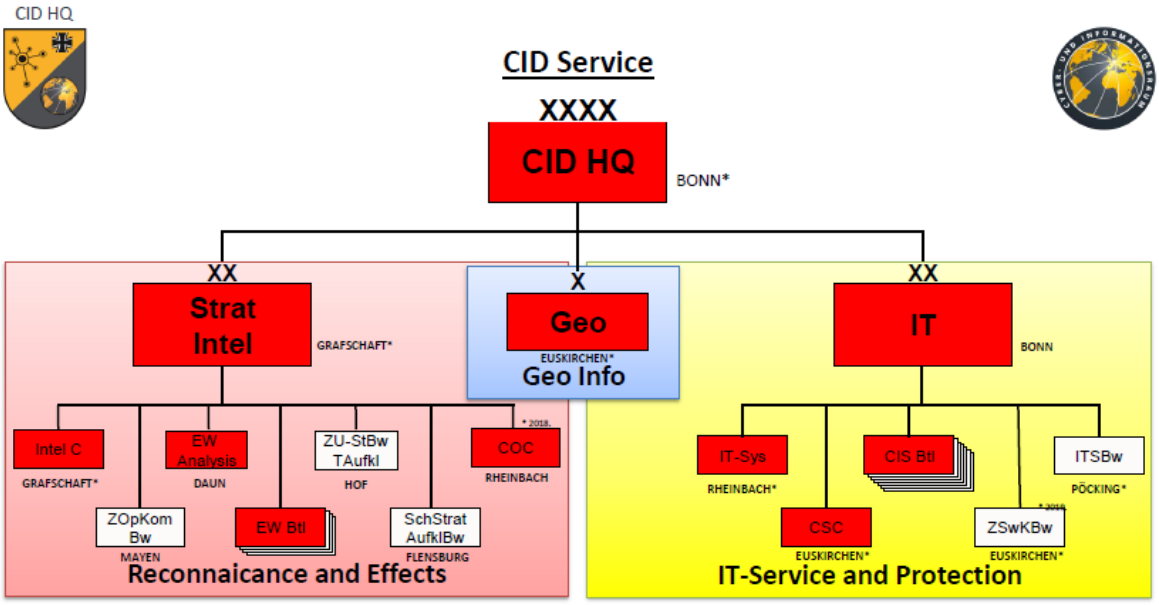


Figura 8 – Estrutura do CID alemão

Fonte: LTC *Chris Hoffmann Wolfram* (2019, p. 20)

4.4. Reino Unido

O Conselho Nacional de Segurança do Reino Unido, em 2010, e após identificar ataques hostis de organismos nacionais pelo ciberespaço, inclui as ciber ameaças no grupo dos riscos que mais ameaçam a segurança nacional, considerando os seus possíveis impactos (Cameron, 2010).

A maioria das reformas organizacionais relativas à cibersegurança no reino Unido, foram realizadas com a adoção da UK *National Cyber Security* (NCSS) de 2009, mas derivado da experiência, foram implementadas alterações organizacionais em determinadas estruturas, com a NCSS de 2011. A estrutura organizacional foi então dividida em três: (i) o *Office of Cyber Security & Information Assurance* (OCSIA); (ii) o *National Security and Intelligence*; e (iii) o *Cyber Defence Centre*, na dependência do Ministério da Defesa (MoD) (UK Government, 2011).

As FFAA do Reino Unido possuem uma visão conjunta do ciberespaço, integrando as áreas do planeamento, treino e até ao cabimento orçamental. O comando das unidades de CD encontram-se na dependência direta do *Joint Forces Command*, de modo a assegurar uma aproximação consistente e holística às operações no âmbito da defesa, desenvolvidas no ciberespaço (UK Parliament, 2013).

Com o principal objetivo de desenvolver e tornar as capacidades de CD mais flexíveis, avançadas e adaptadas ao novo campo de batalha, foi criado o *Defence Cyber Operations*

Group (DCOG) em março de 2015. O seu foco é assegurar que o Reino Unido desenvolve o planeamento, treino, exercício e opera, de forma integrada, as operações de CD com as restantes áreas das operações militares. O DCOG é um constituído por um conjunto de unidades ciber pertencentes à defesa (House of Commons, 2012).

Dessas unidades, destaquei o *Global Operations and Security Control Centre*, que realiza a gestão de um modo integrado, da CD das FFAA e das redes informacionais do MoD, incluindo as redes de teatro. Disponibiliza uma monitorização em tempo real, proveniente de mais de 200 mil sensores distribuídos pelas redes de defesa *world wide web*. Possui também uma capacidade de análise *forensic*, a fim de realizar a atribuição de incidentes cibernéticos, de modo a contribuir para o conhecimento mundial sobre o método e as ferramentas dos grupos, ou indivíduos, que desenvolvem ataques cibernéticos. Com estes indicadores identificados, é possível mitigar vulnerabilidades e ajustar procedimentos de defesa, a fim de melhorar a capacidade de resposta a ataques desenvolvidos no ciberespaço (UK MoD, 2014). De salientar a utilização de *white hackers*, com a finalidade de detetar vulnerabilidades dos próprios sistemas, como apresentado no apêndice C. No mesmo apêndice de referir que Yossi Sassi refere o Reino Unido como um exemplo a seguir na área da CD.

Para a proteção das Infraestruturas críticas, bem como das organizações públicas e privadas, foi criado o *Centre for the Protection of National Infrastructure* (CPNI) em 2007, que desenvolve esforços diretos com o governo do reino Unido, garantindo deste modo o aconselhamento de segurança nas áreas físicas, pessoal, bem como ciber e informacional (CPNI, 2020).

De salientar que a nível de GE o Reino Unido possui, na dependência do Exército, as *Light Electronic Warfare Teams* (LEWT), que se constituem como uma unidade de informações de elite, especializada na recolha e análise das comunicações inimigas. Normalmente são projetadas em conjunto com forças de operações especiais, ou unidades de reconhecimento da 16th *Air Assault Brigade* (Elite UK Forces, 2020).

4.5. Brasil

Até ao ano de 2009 o Brasil tinha a decorrer três programas de grande importância para a estratégia de defesa nacional: (i) o programa espacial; (ii) o programa nuclear; e (iii) o programa cibernético. No mesmo ano, os três programas, foram distribuídos pelos três ramos das FFAA, ficando o programa cibernético à responsabilidade do Exército (Presidência da República, 2012).

Em agosto de 2010 é ativado o núcleo do Centro de Defesa Cibernética (CDCiber), que apenas em 2012 teve a sua criação oficial. A partir de 2017, passa para a dependência do recém criado, Comando de Defesa Cibernética (ComDCiber), integrado na estrutura do Exército, num modelo de organização conjunta, com a participação de militares de todos os ramos das FFAA brasileiras. A missão do ComDCiber é "[…] planear, orientar, coordenar e controlar as atividades operacionais, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética […]", atuando como organismo nacional, central e coordenador, através da monitorização e proteção constante dos sistemas brasileiros de informações, sejam eles militares ou civis. (Ministério da Defesa, 2017).

O governo identificou os riscos associados, tendo criado os organismos necessários, mas a médio prazo, notou-se um desinvestimento, tanto económico, como, principalmente a nível de pessoal e sua respetiva qualificação e experiência. Sendo talvez aqui, o maior entrave à evolução do programa ao longo prazo (Vasquez, 2020).

Com a reponsabilidade da realização de grandes eventos, o Brasil identificou a necessidade de organizar uma estrutura composta por diversos organismos no âmbito da CD, levando a uma evolução do programa Ciber. Destaque para o Rio +20 em 2012, a Taça das Confederações e a jornada mundial da Juventude, ambos em 2013, o Campeonato do Mundo de Futebol, em 2014 e os Jogos Olímpicos em 2016 (Vasquez, 2020).

A figura 9 apresenta o modo como o Brasil se organizou ao nível de CD, durante a jornada mundial da Juventude em 2013.

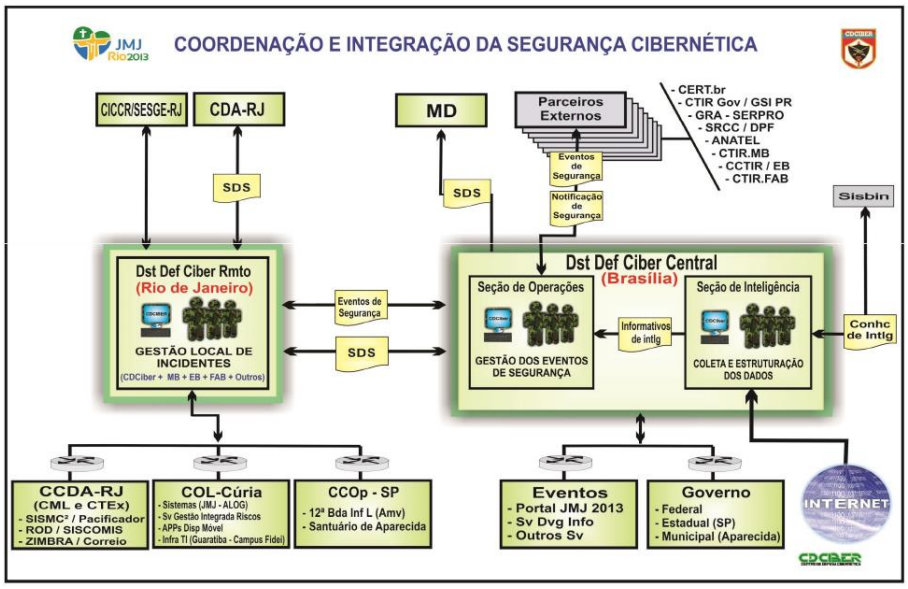


Figura 9 – Estrutura de coordenação Ciber para as Jornada Mundial da Juventude 2013

Fonte: Apresentação realizada no VIII Curso de Extensão de Defesa Nacional (2014)

De salientar a cooperação com entidades civis num ambiente de complementariedade, bem como a relevância atribuída à questão das Informações, materializada pela implementação de um organismo destinado à sua análise e processamento.

Em 2015 foi criado o núcleo da escola nacional de defesa cibernética, em parceria com a universidade de Brasília, cujo objetivo é capacitar engenheiros e profissionais do setor, para o combate a ataques cibernéticos.

A participação de militares do exército brasileiro nas edições do CiberPerseu, levou a que fossem adquiridas experiências e conhecimentos, relacionados principalmente com boas práticas em termos de cooperação e coordenação de entidades militares com entidades civis na área da CD. O exercício Guardião Cibernético, foi exemplo disso, pois tem como grande objetivo, além da criação de oportunidades de treino, a de envolver entidades civis, na troca de conhecimentos e no desenvolvimento de procedimentos conjuntos, num cenário de defesa a um ataque a infraestruturas críticas nacionais, que coloquem em causa a soberania nacional (Vasquez, 2020).

A figura 10 apresenta uma proposta para a estrutura Ciber brasileira, apresentada durante o VIII Curso de Extensão em Defesa Nacional, que decorreu em Belém, de 07 a 11 de abril de 2014.

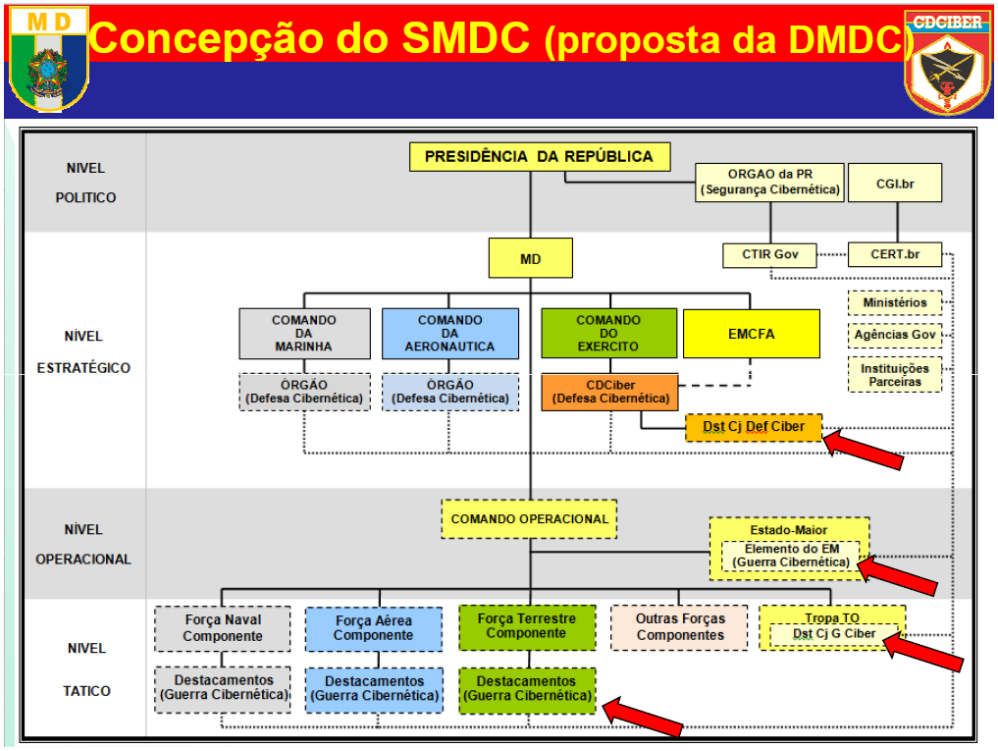


Figura 10 – Proposta para Estrutura Ciber do Brasil

Fonte: Apresentação realizada no VIII Curso de Extensão de Defesa Nacional (2014)

Desta estrutura podemos salientar que, apesar da organização referida anteriormente, que atribui a responsabilidade ao Exército para a coordenação da área Ciber no Brasil, existem ao transversalmente aos vários níveis definidos pela Estratégia, organismos que têm responsabilidades atribuídas e que se encontram interligados entre si. É bastante importante que todos os níveis se encontrem alinhados e coordenados no combate às ameaças cibernéticas, mesmo que, aparentemente se encontrem dependentes de uma unidade inserida numa componente subordinada (CDCiber, 2014).

O Centro de Instrução de Guerra Eletrónica (CIGE), criado em 1984 e atualmente na dependência do Comando de Comunicações de Guerra Eletrónica do Exército, possui uma estreita cooperação com o ComDCiber. Esta, passa muito pela formação, tendo além de outros eventos no passado, desenvolvido um curso de Planeamento de GE e Guerra Cibernética, em 2019, após tendo sido identificada pelo Brasil a relevância da relação entre as áreas de GE e de CD (Governo Brasileiro, 2020).

4.6. Síntese conclusiva

Em suma podemos de um modo geral, identificar algumas tendências no que concerne à necessidade de uma consciência nacional de CD, materializada pela implementação de um organismo responsável pela coordenação e partilha de informação. No que respeito à GE a tendência mais relevante é a da junção com a CD no que se designa por CEMA. Assim é concretizado o OE2 e respondida a QD2. Foi remetido para o apêndice D e E, outros casos também analisados, relegados para segundo plano. E Portugal, qual a nossa realidade nas áreas de CD e de GE?

5. As estruturas de Guerra Eletrónica e de Ciberdefesa em Portugal

O presente capítulo apresenta a situação nacional referente à GE e CD, salientando as estratégias definidas pelo poder político e de que modo as FFAA e, em particular o Exército se alinha com elas.

5.1. Estratégia de Guerra Eletrónica e de Ciberdefesa nacional

A nível nacional no Conceito Estratégico de Defesa Nacional (Governo de Portugal, 2013), são identificadas um grupo de ameaças passíveis de serem efetivadas através do ciberespaço, que poderão afetar infraestruturas críticas de suporte para a sociedade, para a economia e para segurança nacional.

Decorrente da Resolução do Conselho de Ministros n.º36 (ENSC, 2015, p. 3738), Portugal identifica "[…] A necessidade de proteger as áreas que materializam a soberania nacional, assegurando a autonomia política e estratégica do País", e por consequência a carência premente, em estabelecer estruturas e respetivas linha de ação, que permitam minimizar os riscos inerentes ao ciberespaço. O mesmo documento, determina que o CNCS possui a nível nacional "[…] o papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas […]" (ENSC, 2015, p. 3739).

Em março de 2019, o governo aprova em Conselho de Ministros a ENSC, que prevê a sua implementação durante os 4 anos seguintes (CNCS, 2019). As principais linhas de ação da ENSC visam a garantia de proteção e defesa das infraestruturas críticas nacionais, bem como a manutenção de funcionamento dos serviços públicos vitais para os cidadãos e entidades privadas. O produto, agora aprovado, teve o seu início em agosto de 2017 pelo Conselho Superior de Segurança do Ciberespaço, que teve como alicerces a estratégia aprovada em 2015 (CNCS, 2019).

No que respeita a GE, os organismos existem principalmente no seio das FFAA, o que é sustentado pelo próprio conceito, já apresentado. Mesmo assim, da investigação realizada, houve oportunidade de verificar valências semelhantes nas Forças e Serviços de Segurança (FSS), bem como em organismos de Polícia Criminal e Serviços de Informações nacionais.

5.2. O papel do Exército Português nas estruturas de GE e de CD nacionais

A estratégia militar, bem como as suas orientações, focam a área da cibersegurança, na responsabilidade do Conselho de Chefes de Estado-Maior, suportado pelo Centro de Ciberdefesa (CCD) do EMGFA. Em 2013, a Orientação Política para a CD, estipulava medidas que orientavam as Forças Armadas (FFAA) no sentido de implementar um CCD,

que se estabeleceu operacional apenas em 2015. O referido organismo assegura a coordenação das operações no ciberespaço desenvolvidas pelas FFAA com o CNCS. Identifica-se como um elemento estruturante no que respeita a uma eventual resposta nacional a uma ameaça cibernética, visto que detém os meios necessários para apoiar a sociedade civil. O exemplo da série de exercícios CiberPerseu, tem sido um exemplo de melhoria nos processos e procedimentos de cooperação entre a sociedade civil e as FFAA na área da CD.

Considerando a estrutura do Exército, no que respeita à CD, devem ser considerados três níveis: (i) o CCD do EMGFA; (ii) o Departamento de Ciberdefesa e Segurança da Informação (Dep CD SegInfo) da DCSI; e por último (iii) uma capacidade a ser edificada com o projeto em desenvolvimento da CD Tática do Exército "CD-DEPLOY".

O Dep CD SegInfo contribui para a garantia da Informação, nas vertentes de CD e Segurança da Informação. Na sua dependência possui o Núcleo de Segurança da Informação e o Núcleo de Operações em Redes de Computadores (CNO[10]). Através do Núcleo CNO tem a capacidade de planear, coordenar e dirigir investigações de incidentes, bem como partilhar informação com os elementos CIRC nacionais, OTAN ou de outras nações. Pode também deter, prevenir, detetar e recuperar qualquer tipo de incidente/ataque contra os sistemas de informação do Exército, proporcionar resposta a incidentes, aviso e alerta e, por último realizar, caso seja solicitado, testes de penetração e auditorias técnicas destinadas a avaliar o grau de proteção das redes e sistemas de informação (Exército Português, 2013).

No caso da GE, o Centro e Treino de Guerra Eletrónica (CTGE), surge no QO n.º 07.02.22 do RTm, de 15 de fevereiro 2016. Assim, e decorrente do Art.º 501 – Responsabilidades Nacionais, da Publicação do EMGFA (1994), o CTGE contribui para garantir a superioridade de informação, através do desenvolvimento de operações de GE, tendo como capacidades: (i) a recolha e análise de informações acerca de inimigos, ou potenciais inimigos, estabelecidos pelas políticas da OTAN; (ii) o desenvolvimento de doutrina e identificação de procedimentos a tomar durante a condução de operações de GE; (iii) o desenvolvimento de projetos que garantam a capacidade de GE de acordo com os parâmetro definidos pela OTAN, acautelando a manutenção e adequação dos equipamentos à respetiva evolução tecnológica e da ameaça; (iv) a criação de oportunidades de treino que garantam o desenvolvimento dos conhecimentos e experiências dos militares de GE, bem

[10] *Computer Network Operations.*

como apoiar a realização de cursos e simpósios de apoio a exercícios no âmbito da OTAN; (v) desenvolver diligências para garantir a representação de Portugal nas reuniões de GE no âmbito dos compromissos internacionais; e (vi) a recolha e centralização de informação de GE, bem como a manutenção de uma base de dados disponível para a comunidade de GE.

5.3. Análise da estrutura de GE e de CD do Exército

Ao nível dos Elementos da Componente Operacional do Sistema de Forças (ECOSF), de acordo com o Sistema de Forças Nacional de 2014, que precede o despacho N.º 156, do Chefe de Estado-Maior do Exército, de 21 de dezembro de 2015, as unidades que compõe o nível tático de GE e de CD, como representado no figura 11, são: (i) a CompGE, cujas capacidades e possibilidades se encontram vertidas no respetivo QO (09.02.08) de 13Mai15; e (ii) o ModTat CIRC, garantido pela DCSI, mas incluído no QO (09.03.02) do Batalhão de Transmissões, de 15Fev16. De salientar o CTGE se apresenta incluído no QO (07.02.22) de 15Fev16 do RTm.

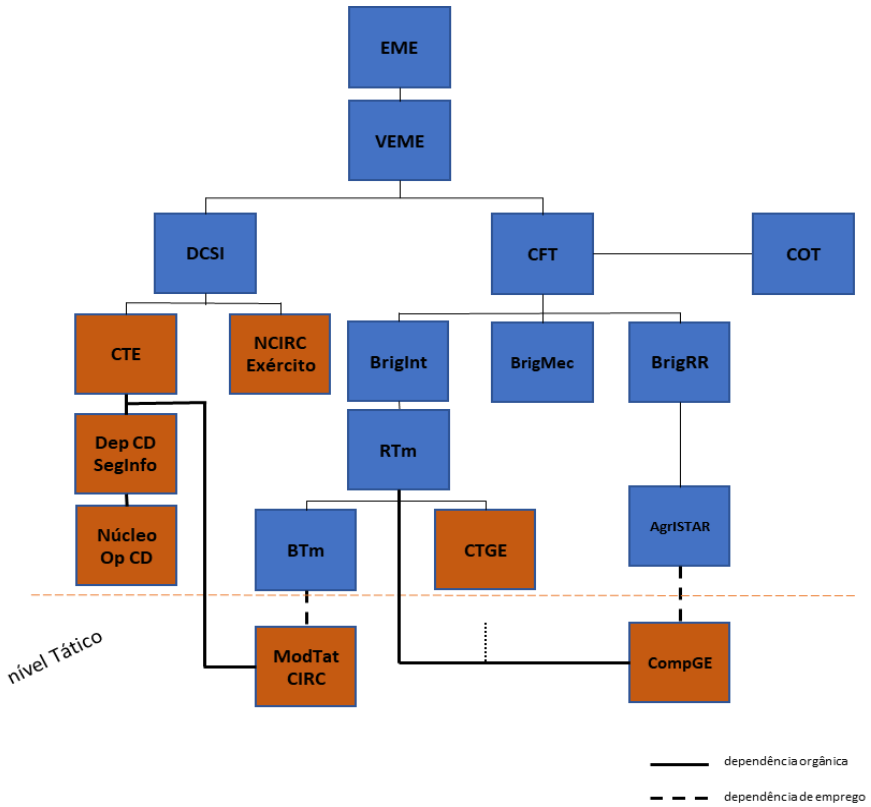


Figura 11 – Estrutura hierárquica das unidades de GE e CD do Exército

Fonte: Adaptado a partir do Despacho N.º 156/CEME (2015)

No que respeito à CD a nível tático, o ModTat CIRC, e de acordo com o apresentado na figura 12, encontra-se subdividido em Seção Integradora (SecInt), Seção Ofensiva

(SecOf) e Seção defensiva (SecDef), que podemos comparar com as três disciplinas da CD já apresentadas anteriormente.

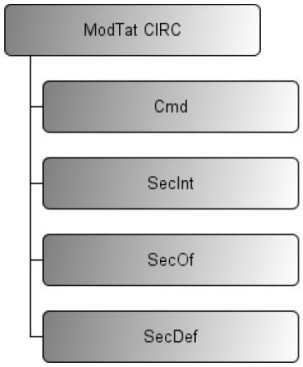


Figura 12 – Estrutura do Módulo Tático CIRC

Fonte: Adaptado a partir do QO 09.03.02 do BTm, Exército Português (2016)

O ModTat CIRC tem como missão assegurar a CD de modo a garantir os sistemas e meios de comunicações disponíveis para as nossas forças, mesmo num ambiente de ataques ciber. As capacidades do ModTat CIRC foram materializadas nas capacidades na área da CD, identificadas para o Dep CD e SegInfo, sendo assegurados pela DCSI, com uma constituição de dois oficiais, quatro sargentos e três praças. Possui viaturas equipadas, de um modo modular, correspondendo a cada seção apresentadas na figura 12. Em caso de emprego em treino ou condução de operações é colocado na dependência do BTm.

Já a CompGE, de acordo com a figura 13, encontra-se dividida por pelotões de GE (PelGE), de apoio ligeiro e de apoio médio.

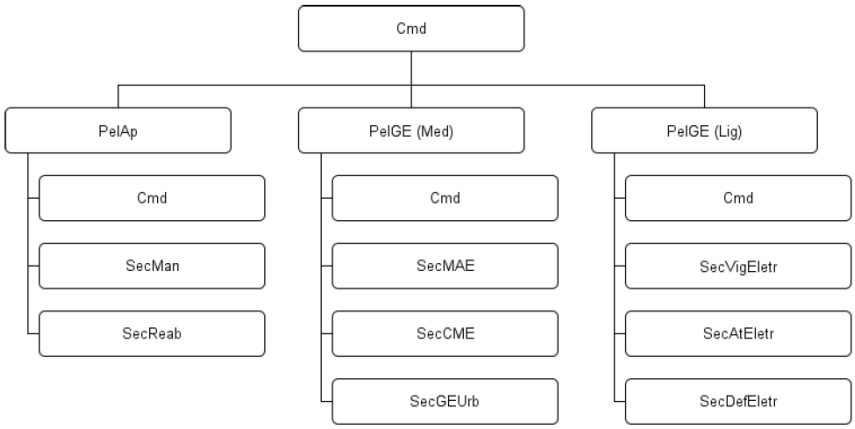


Figura 13 – Estrutura da Companhia de GE

Fonte: Adaptado do QO 09.02.08 da CompGE, Exército Português (2015)

A CompGE tem como capacidades: (i) participar, no esforço nacional de *Signal Intelligence* (SIGINT), através da recolha de dados paramétricos de natureza eletromagnética, para a atualização da Base de Dados de Emissores Nacionais e Bases de Dados internacionais, como exemplo a NEDB da OTAN; (ii) apoiar em ações de GE aos ECOSF, nomeadamente nas áreas da pesquisa, identificação, interceção e radiolocalização de emissões eletromagnéticas e no âmbito das contramedidas eletrónicas, designadamente no empastelamento eletrónico (incluindo GSM, Wi-Fi e Bluetooth), na deceção eletrónica e dos sistemas inibidores de frequência; (iii) apoiar em ações de GE a uma unidade de escalão Brigada, ou a três unidades escalão Batalhão; (iv) contribuir para a proteção de uma força contra engenhos explosivos improvisados ativados por controlo remoto; e (v) integrar, através do Agrupamento *Intelligence, Surveillance, Target Acquisition & Reconnaissance* (AgrISTAR), o sistema de ISTAR em apoio às operações de uma unidade de escalão Brigada. Também para a GE existem especificados, no *Capability Codes and Capability Statements* os requisitos mínimos para esta tipologia de unidade, apresentados no anexo C (Exército Português, 2015). A CompGE não possui atualmente qualquer tipo de relação com o CTGE.

Nos PelGE, podemos encontrar de um modo geral, a organização com base nas disciplinas de GE, anteriormente apresentadas. Podemos inferir que ambas as atividades, podem ser organizadas de um modo modular, a fim de serem empregues nos modernos conflitos, de acordo com a necessidade especifica. A CompGE é atualmente uma unidade orgânica do Agrupamento ISTAR, mas possui a capacidade de atuar de forma isolada em apoio a uma força.

5.4. Síntese conclusiva

Em súmula, no que concerne a Portugal, o CNCS constitui-se como organismo fulcral na CD nacional. Já nas FFAA o edifício hierárquico inicia-se no CCD do EMGFA, que se constitui como ponto de ligação entre os ramos e os organismos civis. No Exército o Dep CD SegInfo é responsável pela CD, enquanto que o CTGE é responsável pela GE. Apresentados que estão os dados recolhidas para a presente investigação, é concretizado o OE3 e respondida a QD3, existindo agora, a carência da análise crítica e cuidada, a fim de atingir o corolário deste estudo.

6. Apresentação e discussão dos resultados

Neste capítulo foi apresentada a comparação dos dados do estudo realizado, bem como a proposta para a estrutura de CD e GE para o Exército português. O quadro 3 apresenta os resultados mais relevantes observados nos casos e estudo e na OTAN.

Quadro 3 – Análise comparativa dos casos de estudo

	EUA	China	Alemanha	Reino Unido	Brasil	OTAN
D	- doutrina própria bastante completa - conceito de CEMA espelhadas no vetor de organização	- conceitos de *information* equiparado a *cyber*	- doutrina OTAN e UE - conceito CEMA - interligação com as Informações		- conceito CEMA	- NEWAC (GE) responsável pela doutrina - GE implementado e em revisão - CD para ratificação pelos EM
O	- US CYBERCOM - ARCYBER *Comando de Component* - *CEMA Teams* em apoio a uma brigada	- SSF em apoio ao PLA equiparadas a um ramo das FFAA	- CD e Intell como tarefa nacional - Kdo CIR Comando de Componente ramo das FFAA	- CPNI - DCOG - GE ligada à Intell	- EXE com encargo nacional - ComDCiber (2017) - CD Ciber (2010)	- *Joint EW Core Staff* na dependência do SHAPE - CyOC - *Cyber Rapid Reaction Teams*
T	- CCDCOE - Exercícios OTAN-UE		- CCDCOE - Exercícios OTAN-UE	- CCDCOE - Exercícios OTAN-UE	- influência do Ciberperseu no Guardião Cibernético	- GE exercícios multinacionais (NEMO) - *Cyber Coalition* e *CMX* - OTAN-UE exercícios (*CYBRID* e *Cyber Europe*)
M						
L		- Xi Jinping controla CCSII		- CD na dependência do *JFC*		- GE e CD controlados pelo SHAPE
P	- ARCYBER 16500		- Kdo CIR 14000 (+1000) FOC (2021) (mil e civis)			
I	- cooperação com entidades civis nacionais e internacionais			- MoD apoia Op Ciber nacionais inter		- CyOC
I						- *Capability Codes and Capability Statements*

A tendência de evolução das redes sem fios, ganha relevância com o aparecimento da 5.ª geração de redes móveis, reforça a necessidade e importância de manter em sincronia e perfeita coordenação ambas as disciplinas, voltando a dar à GE a relevância que lhe é devida. Relevância esta, já evidenciada nos diversos países apresentados nos casos de estudo.

Outra tendência identificada, foi a de organizar estruturas com GE e CD, incluindo áreas ligadas às Informações, pois este tipo de organização apresenta vantagens para a instituição militar, possibilitando a rápida análise de Informações disponíveis tanto no ciberespaço como no espetro eletromagnético. Mesmo assim, de salientar que em apoio a operações, é mantida a modularidade das unidades, a fim de serem empenhados os meios necessários e adequados a cada operação.

De um modo geral, os países entenderam que a batalha desenvolvida no ciberespaço, tem, obrigatoriamente, de ser expandida do âmbito militar para toda a sociedade. Como referido por Dan Smith, diretor do *Stockholm International Peace Research Institute* (SIPRI)[11], numa entrevista disponibilizada no *youtube*, em que, quando aborda o tema da cibersegurança, refere que a resiliência (na área ciber) não é construída numa instituição/organização, é algo que deve estar presente na mente de cada indivíduo, e para que tal aconteça, tem que ser ensinada nas escolas, nas faculdades, na vida (SIPRI, 2020).

Assim, existe a necessidade de possuir um organismo coordenador a nível nacional, que se interligue diretamente com o poder político, no sentido de assegurar que a estratégia nacional é seguida. Foi possível observar casos em que essa responsabilidade, na área da CD, se encontra atribuída à instituição militar, ou noutros, a um organismo civil. Neste aspeto Portugal concentrou no CNCS, que se interliga com o CCD do EMGFA, do mesmo modo que se interliga com as empresas ou outros organismos civis.

No âmbito militar, é identificada a tendência para que a área da CD se constitua como uma componente responsável por desenvolver operações no respetivo domínio operacional, equiparada às restantes componentes. Com a salvaguarda da necessidade de manter cada vez mais a sincronização entre todas, para o desenvolvimento e condução de operações militares.

[11] *Stockholm International Peace Research Institute*, é um instituto internacional independente, dedicado à pesquisa de conflitos armados, bem como ao armamento e desarmamento internacional. Implementado em 1966, disponibiliza dados, análise e recomendações em plataformas *open source*, de interesse público em geral, relevante tanto para investigadores, como para agentes de segurança e defesa (SIPRI, 2020).

Mesmo num mundo interligado em rede, existe a necessidade de possuir equipas de resposta rápida que, com a mobilidade a elas associada, permitam assegurar o cumprimento das missões, que não sejam possíveis de realizar remotamente.

6.1. Proposta de estrutura orgânica de Guerra Eletrónica e de Ciberdefesa para o Exército Português

Identificadas as tendências suportadas pelos estudos de caso, o autor deste estudo passa a apresentar uma proposta organizada segundo os vetores de desenvolvimento identificados para a edificação de uma capacidade militar. Deve ser relembrada a importância de assegurar o cumprimento das orientações dadas pela OTAN no *Capability Codes and Capability Statements*, que estipula os requisitos operacionais de cada tipologia de unidade. No caso da CD, em particular para o CD-DEPLOY é apresentado no anexo B, sendo para a CompGE apresentado em anexo C.

Para esta proposta é importante salientar que na dependência do Comando das Forças Terrestres (CFT), encontra-se o Centro de Operações Terrestre (COT), vocacionado para planear, coordenar e supervisionar, as operações correntes desenvolvidas pelos ECOSF.

Os atuais QO do ModTat CIRC e da CompGE refletem a doutrina de referência anteriormente apresentada, devendo ser evidenciada a questão modularidade já existente, que deverá refletir-se na possibilidade do empenhamento parcial das unidades.

Além disso, a presente proposta focou-se nas estruturas e dependências hierárquicas superiores, de CD e GE no Exército, não abordando apenas o nível tático, pois este encontra-se a ser desenvolvido no projeto em curso, da edificação da *Capacidade de CD Tática do Exército "CD-DEPLOY"*. Salientando que para a proposta de estrutura orgânica, em ambas as áreas, foi entendido que é relevante, observar todo o edifício hierárquico como um sistema conjunto, coordenado e em sincronia.

6.1.1. Doutrina

Apesar de não existir doutrina no Exército para a área de CD, o EMGFA tem vindo durante o último ano a desenvolver um esforço bastante grande no sentido de disponibilizar aos ramos uma estrutura doutrinária superior, baseada nas orientações políticas nacionais, bem como na doutrina de referência. Esta doutrina deverá incluir aspetos desde os níveis estratégico, passando pelo operacional e terminando no nível tático.

O Exército de acordo com o PDE 3-00 Operações de 2012, faz referência as atividades ciber eletromagnéticas, abordadas nesta investigação. De considerar o desenvolvimento de uma PDE destinada a CD, outra à GE e uma especifica destinada às CEMA.

6.1.2. Organização

A figura 14 materializa num organograma a proposta desenvolvida por este estudo.

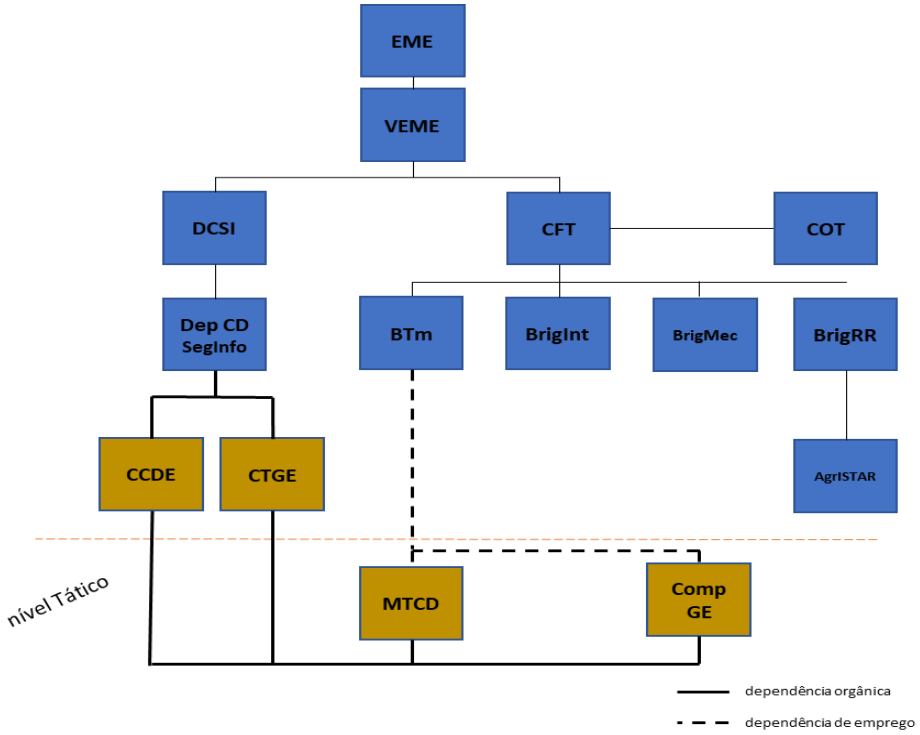


Figura 14 – Estruturas da de CD e GE propostas

Em substituição do atual Núcleo CIRC do Exército, criar um Centro de CD do Exército (CCDE), na dependência do Dep CD SegInfo. Este centro seria reorganizado consoante as disciplinas e valências anteriormente identificadas para a CD, de modo a concentrar os meios de CD. Na sua dependência orgânica, em apoio, fica o Módulo Tático de CD com nova designação de Módulo Tático de CD (MTCD[12]), com equipas prontas a ser projetadas na resolução de incidentes identificados nas redes do Exército, numa missão equiparada às *NATO Cyber Reaction Teams*, em operações exclusivamente defensivas.

No que respeito às operações ofensivas, devem ser restringidas ao CCDE, a fim de garantir, não só o enquadramento operacional e legal, mas também a coordenação com os restantes níveis da estratégia nacional.

No caso da GE, o CTGE é colocado na dependência orgânica do Dep CD SegInfo. Por sua vez, a CompGE é colocada na dependência do CTGE.

Quando em emprego tático para treino ou condução de operações, e considerando a questão e modularidade, são atribuídos ao BTm, os módulos necessários para o cumprimento

[12] Designação das unidades de CD-DEPLOY no projeto da edificação da Capacidade de CD Tática no Exército.

da missão, sejam eles de CD ou de GE. Em apoio, é reforçado o G6 do CFT, com um oficial de CD e outro de GE, para servir de elo de ligação com as respetivas componentes táticas. O COT em coordenação com o G6 do CFT, planeia e coordena as CEMA a desenvolver em apoio a unidades escalão batalhão ou brigada, consoante a situação.

Os centros em questão deveriam possuir uma capacidade permanente, de modo a manter a realização de tarefas diárias nas redes implementadas e permanentes do Exército, sejam elas no aspeto do ciberespaço ou no espetro eletromagnético.

6.1.3. Treino

O treino e formação é assegurado em coordenação com o EMGFA, bem como com os restantes ramos, de modo a maximizar as oportunidades de treino, disponibilizadas pelos exercícios nacionais e internacionais. Essa inclusão deverá, sempre que possível iniciar-se logo desde a fase de planeamento dos exercícios.

Neste sentido, e na área da CD, é de salientar a necessidade de manter, e mesmo até de melhorar, o nível de participação nacional no CCDCOE em Tallinn. No que respeito à GE, promover os contatos entre ramos a nível nacional e dentro das alianças anteriormente referidas a nível internacional.

6.1.4. Material

A OTAN identifica o material necessário para uma capacidade de CD-DEPLOY, estando já materializado no projeto em desenvolvimento relativo à edificação da Capacidade de CD Tática no Exército. O referido projeto prevê o reequipamento das atuais viaturas do ModTat CIRC, encontrando-se alguns equipamentos já adjudicados e os restantes previstos na Lei de Programação Militar de 2019.

Já na área de GE, existe a necessidade premente de atualizar todo o material à carga da CompGE, sendo para tal necessário o desenvolvimento de um projeto semelhante ao da CD, de acordo com os requisitos previstos no anexo C.

No que respeita às plataformas móveis a serem usadas, encontra-se também já previsto, além das três viaturas do ModTat CIRC existentes, consideradas para apoio a equipas de reação rápida e de resposta a incidentes, a inclusão de duas viaturas táticas com *Shelter*.

6.1.5. Liderança

A arma de Transmissões, bem como os seus militares, continuam a assegurar o preenchimento das necessidades em ambas as áreas no Exército. Manter a ligação hierárquica de complemento e coordenação com o CCD do EMGFA.

Sendo assim, é de grande importância a consciencialização das entidades responsáveis, para que sejam garantidas as condições, financeiras, ou outras, para que as referidas capacidades sejam implementadas do modo operacional que garanta as responsabilidades nacionais perante as alianças.

6.1.6. Pessoal

Este é o vetor de desenvolvimento mais crítico que temos de avaliar, pois o pessoal destinado às áreas em questão, considerando o conhecimento e experiência que necessitam de adquirir, deve ter a possibilidade de possuir uma carreira num carater excecional.

O ideal seria que desde o início da carreira passassem pelas funções mais básicas, fossem adquirindo conhecimento por intermédio dos diversos cursos e oportunidades de treino, possibilitando o acompanhamento do evoluir das tecnologias e procedimentos em questão. Deste modo seria rentabilizado o tempo investido pela instituição e pelos militares, a fim de possibilitar a edificação de unidades de excelência nestas áreas tão técnicas que tanto exigem em termos de aprendizagem.

Esta situação não se coaduna com aspetos previstos nas regras de colocação do pessoal, atualmente em uso no Exército, devendo ser criados mecanismos de exceção que protejam os militares e a própria instituição.

Os QO de pessoal dos CCDE e do CTGE, deveriam ser redimensionados de modo possibilitar o cumprimento das capacidades identificadas para cada um deles.

6.1.7. Infraestruturas

As infraestruturas para a GE situadas no RTm no Porto, são adequadas ao efeito atualmente em uso pelo CTGE e pela CompGE, devendo ser pensado algo semelhante para o caso do CCDE. Assim sendo, deve a DCSI continuar a organização do atual edifício pertencente ao Núcleo de SegInfo e ao Núcleo CNO, para a implementação do CCDE. Não sendo possível neste edifício, identificar nova localização que cumpra requisitos necessários. O mesmo se deve acautelar para o armazenamento e parqueamento de material e viaturas.

De salientar que a questão de dependência orgânica não implica efetivamente a deslocalização geográfica, tal como podemos observar com os ModTat CIRC atuais. Assim sendo a CompGE, apesar da presente proposta incluir a sua alteração de dependência, não iria ser deslocalizada das suas atuais infraestruturas.

6.1.8. Interoperabilidade

Este vetor é garantido pelo *Capability Codes and Capability Statements* da OTAN, sendo assim importante segui-lo a nível nacional, no âmbito militar. Além disso, também se

encontra acautelado no projeto da edificação da Capacidade de CD tática no Exército, a aquisição de meios utilizados no SIC-T, e na sua interoperabilidade com os respetivos sensores de CD.

O quadro 4 apresenta a comparação entre a estrutura atual e a proposta realizada, salientando as alterações mais significativas.

Quadro 4 – Comparação entre as estruturas atuais e a proposta apresentada

	Estrutura orgânica atual	**Estrutura Orgânica proposta**
D	- esforço do EMGFA em materializar o edifício doutrinário na área da CD - não existe doutrina nacional no Exército	- Desenvolver 3 PDE: (i) CD; (ii) GE; e (iii) CEMA
O	- Dep CD SegInfo = > Núcleo CNO => ModTat CIRC - ModTat CIRC emprego tático na dependência do BTm - AgrISTAR => ComGE - CompGE sem qualquer dependência do CTGE	- Dep CD SegInfo => CCDE => MTCD - Dep CD SegInfo => CTGE => CompGE - emprego tático: COT/CFT => módulos do MTCD e da CompGE em coordenação do G6 CFT reforçado
T	Assegurado em coordenação com o EMGFA	
M	*Capability Codes and Capability Statements* da OTAN, com atenção às plataformas	
L	Arma de Transmissões	
P	- além do pouco pessoal as normas de nomeação e colocação do pessoal obrigam à rotação de militares especializados	- acautelar a possibilidade de uma carreira de caráter excecional - adequar QO CCDE e CTGE
I	- DCSI => Dep CD SegInfo e ModTat CIRC - RTm => CTGE e ComGE	- DCSI desenvolve o CCDE - RTm => mantém infraestruturas de GE
I	*Capability Codes and Capability Statements* da OTAN	

6.2. Síntese conclusiva

Em síntese, o projeto de CD-DEPLOY em progresso apresenta-se como uma boa evolução na CD do Exército, mas urge uma reorganização ao edifício hierárquico das CEMA. Neste sentido a junção na unidade mãe da arma de Transmissões, e especificamente

no Dep Seg Info, aparenta uma evolução natural, que exige uma adaptação nos restantes vetores relacionados com a edificação de uma capacidade militar.

7. Conclusões

The quieter you become, the more you are able to hear

Jalal ad-Din Muhammad Rumi (1207-1273)

A sociedade contemporânea encontra-se cada vez mais apoiada e dependente da tecnologia, nomeadamente no que respeita à interconexão garantida pelas redes. Estas, para manterem a ligação entre si, precisam de um meio de transmissão, também este bastante associado à evolução tecnológica. O conceito de redes sem fios, obrigou a que a transmissão se suportasse do espetro eletromagnético, também em proveito da utilização do ciberespaço. Quem tiver ao seu dispor as capacidades que permitam controlar ambos os domínios, tão interligados, terá na sua posse, uma vantagem deveras desejável por todos. Esta ideia encontra-se bastante suportada pelos textos apresentados nos anexos D e E.

O objeto deste estudo centra-se nas capacidades de GE e a CD no Exército Português. Para tal, foi identificado o estado atual das estruturas, bem como da estratégia definida a nível nacional, e salientada a importância da reorganização da estrutura no Exército. Em áreas tão especificas e técnicas como as apresentadas, houve uma premente necessidade de constituir um quadro de referência que orienta o estudo, para tal foi utlizada documentação da OTAN e nacional, que se encontra versada em documentos legislativos e oficiais. Foi apresentada a realidade atual de diversos países, a fim de identificar tendências, nos casos de estudo.

O procedimento metodológico utilizado recorreu a um raciocínio indutivo, tendo sido realizada uma comparação com base nos vetores de edificação de uma capacidade militar. O desenho de pesquisa a utilizado foi o caso de estudo, numa ótica de *bench leaning*, a fim de apresentar uma proposta da estrutura orgânica de GE e de CD para o Exército Português.

Na cimeira de Bruxelas em 2018, os países aliados, concordaram com a ativação de um novo CyOC, na Bélgica, fortalecendo deste modo a estrutura de Comando da OTAN e garantindo uma *situational awareness* atualizada, bem como, garantindo a coordenação operacional de todas as atividades neste domínio. Em fevereiro de 2019, foram enviadas linhas orientadores para os países membros, identificando um vasto número de ferramentas, a fim de que, também os próprios países tenham a possibilidade de fortalecer as suas capacidades.

Na dependência do CyOC encontram-se as *Cyber Rapid Reaction Teams*, que têm como principal foco a proteção das próprias redes presentes no ciberespaço. Estas equipas

são constituídas por um número reduzido de elementos, organizadas de um modo modular, disponíveis 24/7 e projetáveis. No que respeito à GE a OTAN, como aliança de índole militar que é, possui, através do seu NEWAC, um organismo responsável pelo desenvolvimento da sua política, doutrina e respetivos conceitos de C2.

Existe um esforço de cooperação OTAN-UE, que tem vindo a evidenciar as questões relacionadas com o ciberespaço, obrigando a que os estados-membros se comprometam a reforçar as suas capacidades nesta área, nomeadamente no investimento em vetores como a formação e treino. A visão da UE segue no sentido de manter, os estados-membros informados e com o conhecimento das ameaças. A UE acompanha a OTAN na sua parceria de cooperação e complementaridade.

Considerando os casos de estudo apresentados, podemos identificar algumas tendências, no que respeito à organização das estruturas de GE e de CD. Não só as referidas áreas, se encontram a desenvolver atividades conjuntas, mas também estruturas da área de Informações se aproximam cada vez mais. No âmbito militar, é identificada a tendência para que a área da CD se constitua como uma componente equiparada às restantes componentes das FFAA, que se destinam a desenvolver operações no seu respetivo domínio operacional.

No nível militar o CCD do EMGFA, identifica-se como um elemento estruturante no que respeita a uma eventual resposta nacional a uma ameaça cibernética, interligando-se diretamente como o CNCS, e em simultâneo, com a área de CD de cada um dos ramos das FFAA. No que respeita ao Exército, cabe ao Dep CD SegInfo e ao Núcleo CIRC do Exército, na dependência da DCSI, essa ligação. Por sua vez este departamento coordena, em cooperação com o BTm, as ações desenvolvidas na área defensivas da CD no Exército português. Já no que respeita à GE, a CompGE, estabelecida no Porto, e na dependência do AgrISTAR, encontra-se responsável por desenvolver ações de treino e formação.

Com base na doutrina desenvolvida pelas alianças, apresenta-se como uma necessidade de que seja constituído um edifício doutrinário nacional, nomeadamente na área da CD. No aspeto nacional, deverá ser considerada a necessidade de desenvolver três PDE: (i) CD; (ii) GE; e (iii) CEMA.

Os QO dos CCDE e do CTGE devem ser desenvolvidos, na dependência do Dep de CD SegInfo, considerando o aspeto de modularidade de cada uma das áreas. Os centros em questão deveriam possuir uma capacidade permanente, de modo a realizar as tarefas diárias nas redes implementadas e permanentes do Exército, possuindo equipas modulares, a fim de garantirem uma resposta imediata a incidentes, bem como a serem empenhadas no treino e

condução de exercícios. De grande relevância, importa distinguir as operações defensivas e as ofensivas, pois em concordância com OTAN, existe uma necessidade extrema de garantir que as operações ofensivas são controladas aos mais altos escalões de responsabilidade.

Para o material necessário de adquirir em ambas as áreas, é extraordinariamente importante cumprir com o identificado pela OTAN para a ambas as capacidades. No que respeita ao CD-DEPLOY, encontra-se acautelado pelo projeto em curso da edificação da Capacidade de CD tática do Exército, sendo urgente o desenvolvimento de um projeto semelhante para a GE.

Urge a necessidade de avaliar a possibilidade de estabelecer uma carreira de carater excecional para os militares que almejem desempenhar tarefas nestas áreas, possibilitando rentabilizar o investimento da instituição e trabalhar no sentido e alcançar unidades de excelência em áreas tão técnicas como as apresentadas.

A interoperabilidade é garantida pelo *Capability Codes and Capability Statements*, normalizando as questões relacionadas com o material. Os procedimentos serão normalizados com o treino e posterior desenvolvimento de SOP ou TTP para as respetivas unidades.

Com tudo o anteriormente em pensamento, é proposto uma estrutura orgânica de GE e de CD para o Exército Português, respondendo desta forma à QC, identificada para a investigação: *Que tipo de estrutura de GE e de CD, para o Exército Português, melhor se integra no seio das alianças a que Portugal pertence?*

Quanto à questão de manter a GE e CD separadas ou não, eu diria que, considerando a evolução da tecnologia, seria sem dúvida de unir de um modo complementar, acautelando o seu empenhamento conjunto em treino ou condução de operações. Esta união é materializada no Dep CD SegInfo da DCSI, podendo ser potenciada com o desenvolvimento da doutrina das CEMA

É importante que sejam desenvolvidos estudos que investiguem a importância de associar a área das Informações aos organismos que irão desenvolver as CEMA. Os casos de estudo da China e da Rússia em apêndice E, apresentaram-se bastante desafiantes, graças não apenas à barreira linguística, mas também relacionado com a evolução já conseguida. Seria interessante desenvolver um estudo aprofundado sobre estes dois casos de estudo. Também a questão da distinção que se nos exige de distinguir as operações de CD ofensivas e defensivas carece de uma proposta de estudo

A arma de transmissões, na sua história, foi identificada como arma e não como um serviço pelo aspeto de possuir a capacidade de desenvolver operações de GE. Algo que foi ligeiramente controverso, principalmente, desde que, o Exército, ao longo dos tempos, tem vindo a abandonar o seu empenamento e por consequência o seu investimento nesta área. Com o surgimento da CD a arma de transmissões ganha uma nova importância e, por conseguinte, uma grande responsabilidade no campo de batalha, que terá de demonstrar estar à altura de o desempenhar.

There are two types of companies: those that have been hacked,
and those who do not know they have been hacked
Robert Mueller, diretor do FBI (2012)

Referências Bibliográficas

Academia Militar. (16 de maio de 2019). *5th NATO CYBER DEFENCE - SMART DEFENCE PROJECTS' (CD SDP) CONFERENCE*. Obtido em 03 de maio de 2020, de Academia Militar: https://academiamilitar.pt/5th-nato-cyber-defence.html

ARCYBER. (2020). US Army Cyber Command. Obtido em 27 de março de 2020, de https://www.arcyber.army.mil/

Burenok, V., Kravchenko, A., & Smirnov, S. (09 de outubro de 2009). Curso - em um sistema de armas centrado na rede. Obtido em 26 de abril de 2020, de http://www.vko.ru/koncepcii/kurs-na-setecentricheskuyu-sistemu-vooruzheniya

Cameron, D. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* Obtido em 09 de abril de 2020, de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

CCDCOE. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations.* New York: Cambridge University Press.

CCDCOE. (2020). Theoretical Offensive Cyber Militia Models. Tallinn. Obtido em 04 de maio de 2020, de https://ccdcoe.org/library/publications/theoretical-offensive-cyber-militia-models/

CDCiber. (2014). Perspectivas em face da espionagem eletrónica. *VIII Curso de Extensão em Defesa Nacional.* Belém/PA. Obtido em 24 de abril de 2020

CEME. (21 de dezembro de 2015). Despacho N.º 15/CEME/2015. Lisboa.

Cendoya, A. (2016). *National Cyber Security Organisation: Spain.* Tallinn.

CloudFlare. (2020). What is a Denial-of-Service (DoS) Attack? Obtido em 04 de maio de 2020, de https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

CNCS. (23 de março de 2019). Governo aprova nova Estratégia Nacional de Segurança do Ciberespaço. Obtido em 23 de março de 2020, de https://www.cncs.gov.pt/recursos/noticias/governo-aprova-nova-estrategia-nacional-de-seguranca-do-ciberespaco/

COR Baltazar, A. (2018). *RFI - Ciberdefesa.* Gabinete do Adido de Defesa em Berlim.

COR Baltazar, A. (2019). *Visita ao Ramo/Comando alemão CIBER.* Gabinete do Adido de Defesa em Berlim.

Costello, J. (20 de janeiro de 2016a). China Finally Centralizes Its Space, Cyber, Information Forces. Obtido em 24 de abril de 2020, de https://thediplomat.com/2016/01/china-finally-its-centralizes-space-cyber-information-forces/

Costello, J. (08 de fevereiro de 2016b). The Strategic Support Force: China's Information Warfare Service. Obtido em 24 de abril de 2020, de https://jamestown.org/program/the-strategic-support-force-chinas-information-warfare-service/

Council of the European Union. (14 de novembro de 2016). Implementation Plan on Security and Defense. Obtido em 01 de março de 2020, de https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf

CPNI. (2020). *CPNI - About*. Obtido em 24 de abril de 2020, de https://www.cpni.gov.uk/about

CyberArt. (2018). *The art of Cyber Security*. Obtido em 25 de abril de 2020, de https://cyberartsecurity.com/

Cybrary. (2020). What is Forensic Analysis? Obtido em 04 de maio de 2020, de https://www.cybrary.it/blog/2019/02/ok-google-forensic-analysis/

Defending Russia. (2016). EXERCÍCIOS ESPECIAIS "ELECTRON-2016" SÃO REALIZADOS NO SUL DA RÚSSIA. Obtido em 26 de abril de 2020, de https://defendingrussia.ru/a/cpecialnyje_uchenija_elektron2016_prohodjat_na_juge_rossii-6207/

Elite UK Forces. (2020). Light Electronic Warfare Teams. Obtido em 25 de abril de 2020, de https://www.eliteukforces.info/intel/lewt/

EMGFA. (24 de novembro de 1994). PEMGFA - Política de Guerra Eletrónica para as Forças Armadas.

EU. (2013). *Cybersecurity Strategy of the European Union.*

EU. (2018). *Operational Guidance for the EU's international cooperation on cyber capacity building.*

Exército Português. (2012). *PDE 3-00 Operações.* Lisboa.

Exército Português. (08 de julho de 2013). Quadro Orgaânico 14.2.04 - Direção de Comunicações e Sistemas de Informação (DCSI). Lisboa.

Exército Português. (13 de maio de 2015). Quadro Orgânico 09.02.08 - Companhia de Guerra Eletrónica (CompGE).

Exército Português. (15 de fevereiro de 2016). Quadro Orgânico 09.03.02 - Batalhão de Transmissões (BTm).

Gibson, W. (1984). *Neuromancer* (1ª ed.). Nova Iorque: Ace Books.

Gobierno de España. (2013). Estrategia de Seguridad Nacional - Un proyeto compartido. Obtido em 08 de abril de 2020, de https://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

Gobierno de España. (2014). *Informe Anual de Seguridad Nacional.* Obtido em 08 de abril de 2020, de http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf

Governo Brasileiro. (20 de janeiro de 2020). Centro de Instrução de Guerra Eletrónica. Obtido em 24 de abril de 2020, de http://www.ccomgex.eb.mil.br/index.php/centro-instrucao-guerra-eletronica

Governo de Portugal. (2013). *Conceito Estratégico de Defesa Nacional.* Lisboa. Obtido em 25 de janeiro de 2020, de https://www.idn.gov.pt/conteudos/documentos/CEDN_2013.pdf

Headquarters, Department of the Army. (2014). *FM 3-38 - Cyber Electromagnetic Activities.*

Honorato, M. C., Santos, L. F., & Mateus, R. M. (2017). *O Ciberespaço como 5º Domínio Operacional. Impacto Estratégico na Política de Defesa Nacional.* IUM.

House of Commons. (2012). *Defence and Cyber-security - written evidence.* Obtido em 24 de abril de 2020, de https://publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/1881.pdf

InformNapalm. (16 de março de 2020). *Os sistemas de guerra electrónica russos em Donbass têm aparecido com maior frequência em fotografias*. Obtido em 03 de maio de 2020, de International Volunteer Community: https://informnapalm.org/pt/os-sistemas-de-guerra-electronica-russos-em-donbass/

JADL. (15 de junho de 2011). STUXNET - Anatomy of a Computer virus. Obtido em 10 de abril de 2020, de https://jadl.act.nato.int/ILIAS/ilias.php?baseClass=ilSAHSPresentationGUI&ref_id=4295

Kabasakal, C. Z. (2019). The 107th NATO Electronic Warfare Advisory Committee (NEWAC) convenes in Brussels. Obtido em 16 de dezembro de 2019, de https://www.nato.int/cps/en/natolive/news_171280.htm?selectedLocale=en

kaspersky. (2020). *What is Zero Day Exploit?* Obtido em 25 de abril de 2020, de kaspersky: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Khudoleev, V. (14 de abril de 2014). Troops for combat on airwaves.

Kwong, J. (2012). State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining. *Report on China and Cybersecurity*, pp. 30-32.

Ley 36/2015, de 28 de septiembre. (29 de setembro de 2015). Boletín Oficial del Estado. Obtido em 08 de abril de 2020, de https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf

Lindsay, J. (2012). *China and Cybersecurity: Political, Economic, and Strategic Dimensions.* University of California, San Diego. Obtido em 24 de abril de 2020, de http://www.bdo3c.f-sc.org/archives/921.pdf

livejournal. (2016). A nova 19.ª brigada de guerra eletrônica no Distrito Militar do Sul. Obtido em 26 de abril de 2020, de https://bmpd.livejournal.com/1852552.html

LTC Wolfram, C. H. (14 de fevereiro de 2019). German perspective on Cyberspace. *Apresentação Powerpoint no CPOLC VIII*. Tallinn.

McAfee. (13 de dezembro de 2019). 9 Tipos de hackers e suas motivações. Obtido em 25 de abril de 2020, de https://www.mcafee.com/blogs/languages/portugues/9-tipos-de-hackers-e-suas-motivacoes/

McDermott, R. (2017). *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic.* International Centre for Defence and Sevurity.

Ministério da Defesa. (27 de abril de 2017). Comando Conjunto na Defesa Cibernética. Obtido em 24 de abril de 2020, de https://www.defesa.gov.br/noticias/30417-comando-conjunto-na-defesa-cibernetica

NATO. (16 de novembro de 2011). Electronic warfare. Obtido em 26 de março de 2020, de https://www.nato.int/cps/en/natohq/topics_80906.htm?

NATO. (2012). AJP-3.6 - Allied Joint Doctrine for Electronic Warfare.

NATO. (2015). *ATP - 3.6.2 - Electronic Warfare in the Land Battle.*

NATO. (2016). *Bi-SC Capability Codes and Capability Statements.*

NATO. (2017 Draft). AJP-3.20 - Allied Joint Doctrine for Cyberspace Operations.

NATO. (2018). *AAP-06.* NATO Standardization Office.

NATO. (11 de julho de 2018). BRUSSELS SUMMIT DECLARATION. Obtido em 17 de abril de 2020, de https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20180713_180711-summit-declaration-eng.pdf

NATO. (20 de novembro de 2019). Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain. Obtido em 17 de abril de 2020, de https://www.nato.int/cps/en/natohq/news_171028.htm

NATO. (18 de novembro de 2019). Joint Press Point. Obtido em 25 de março de 2020, de https://www.nato.int/cps/en/natohq/opinions_170912.htm?selectedLocale=en

NATO. (31 de outubro de 2019). NATO ships test next generation of electronic warfare defences. Obtido em 26 de março de 2020, de https://www.nato.int/cps/en/natohq/news_169952.htm?selectedLocale=en

NATO. (26 de novembro de 2019). The 107th NATO Electronic Warfare Advisory Committee (NEWAC) convenes in Brussels. Obtido em 26 de março de 2020, de https://www.nato.int/cps/en/natolive/news_171280.htm?selectedLocale=en

NATO. (17 de março de 2020). Cyber defence. Obtido em 2020 de março de 25, de https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

NCI Agency. (2016). *DEPLOYABLE CYBER DEFENCE REFERENCE CAPABILITY.*

Neto, R. B. (2017). *Guerra Cibernética / Guerra Eletrónica - Conceitos, Desafios e espaços de interação.* Obtido em 26 de março de 2020, de https://periodicos.ufpe.br/revistas/politicahoje/article/view/9180

Nunes, P. V. (2015). *Sociedade em Rede, Ciberespaço e Guerra de Informação* (2.ª ed.). Lisboa: Instituto de Defesa Nacional. Obtido em 20 de novembro de 2019, de https://www.idn.gov.pt/index.php?mod=1331&cod=34#sthash.zBd2SEj2.dpbs

Presidência da República. (2012). *Livro Branco de Defesa Nacional.*

Priberam. (2020). Priberam Dicionário. Obtido em 17 de abril de 2020, de https://dicionario.priberam.org/

Raud, M. (2016). *China and Cyber: Attitudes, Strategies, organisation.* Tallinn.

Resolução do Conselho de Ministros n.º 36/2015. (12 de junho de 2015). *Estratégia Nacional de Segurança no Ciberespaço*, Diário da república, 1.ª série - N.º 113, 3738-3742. Lisboa: Presidência do Conselho de Ministros. Obtido em 23 de março de 2020, de https://www.cncs.gov.pt/content/files/rcm_36-2015.pdf

Resolução do Conselho de Ministros n.º 92/2019. (05 de junho de 2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*, Diário da República n.º 108/2019, Série I, 2888 - 2895. Lisboa. Obtido em 04 de março de 2019, de https://dre.pt/web/guest/home/-/dre/122498962/details/maximized

Rios, M. (Realizador). (2016). *Guerra Cibernética, o novo campo de batalha no século 21* [Filme]. Obtido em 21 de abril de 2020, de https://www.youtube.com/watch?v=YqO55dXk-oo&list=PLHU9D8D3exmVqD8qCBVKOnQsawHLZcZMr&index=2

Rios, M. (Realizador). (2018). *Cyberwarfare, porque um hacker pode ser mais perigoso do que uma bomba atômica!* [Filme]. Obtido em 14 de abril de 2020, de https://www.youtube.com/watch?v=eg7sUvn_XIk

Sá, A., Machado, R., & Almeida, N. (janeiro/abril de 2019). O encontro da Guerra Cibernética com as Guerras Eletrónica e Cinética no âmbito do Poder Marítimo. *Revista Escola de Guerra Naval, 25*, 89-128. doi:10.21544/1809-3191.v25n1.p89-128

Sanchéz, C. J. (2018). Evolución del concepto de Ciberdefensa. *Jornadas de Ciberdefesa 2018 del Mando COnjunto de Ciberdefensa.* Madrid.

Sassi, Y. (2020). A Hacker Mindset. *Seminário "A Ciberguerra: como travar e vencer num conflito global"*. Lisboa.

Signal. (06 de agosto de 2018). Army CEMA Teams Advance Information, Electronic and Cyber Warfare. Obtido em 25 de abril de 2020, de https://www.afcea.org/content/army-cema-teams-advance-information-electronic-and-cyber-warfare

Silyuntsev, V., Demin, V., & Prokhorov. (2016). Combat application of EW. Obtido em 26 de abril de 2020, de http://sc.mil.ru/files/morf/military/archive/AC_07_2016.pdf

SIPRI. (2020). About SIPRI. Obtido em 18 de abril de 2020, de https://www.sipri.org/about

SIPRI. (26 de março de 2020). Peace Points: COVID-19, conflict and the future. Estocolmo. Obtido em 18 de abril de 2020, de https://www.youtube.com/watch?v=R7qAAGw7byI&t=27s

Thomas, T. (2012). Three Faces of the Cyber Dragon. *Foreign Military Studies Office*, pp. 69-72.

UK Government. (2011). *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.* Obtido em 09 de abril de 2020, de

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

UK Ministry of Defence. (2013). *Red Teaming Guide.* Londres.

UK MoD. (01 de abril de 2014). Supplementary written evidence. Obtido em 24 de abril de 2020, de https://www.parliament.uk/Documents/commons-committees/defence/mod-and-dh-(MIL0038).pdf

UK Parliament. (22 de março de 2013). Defence and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13 - Defence Committee. Obtido em 24 de abril de 2020, de https://publications.parliament.uk/pa/cm201213/cmselect/cmdfence/719/71904.htm

US Army. (2007). *Army Electronic Warfare Operations for the Future Modular Force 2015-2024.*

US DoD. (18 de agosto de 2017). DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command. Obtido em 31 de março de 2020, de https://www.defense.gov/Explore/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/

USCYBERCOM. (2020). US Cyber Command. Obtido em 27 de março de 2020, de https://www.cybercom.mil/

Vasquez, T. (2020). A experiência brasileira em atuação colaborativa para a segurança cibernética nos Jogos Olímpicos Rio 2016. *Seminário "A Ciberguerra: como travar e vencer num conflito global".* Lisboa. Obtido em 24 de abril de 2020, de https://www.emgfa.pt/noticias/DocumentosRelacionados/2020/SeminarioACiberguerra/documentos/ApresentacaoSeminarioCiberguerra-TCLacerda.pdf

Vass, B. G. (2019). Cyberspace Operations Centre: A Capability User Perspective. *5th NATO Cyber Defence Smart Defence Projects' Conference: Cyber NATO-EU Cooperation.* Lisboa. Obtido em 30 de abril de 2020, de https://academiamilitar.pt/images/site_images/5th_NATO_Cyber_Defence/8_Brigadier_General_HUN_Army_Sandor_VASS_Director_Cyberspace_Operations_Centre_ACO_-_CyOC.pdf

Yasar, N., Yasar, F. M., & Topcu, Y. (2012). Operational advantages of using Cyber Electronic Warfare (CEW) in the batlefield. *Cyber Sensing 2012.* International Society for Optics and Photonics, 2012. doi:https://doi.org/10.1117/12.919454

Anexo A — Atos de Guerra Cibernética - exemplos

Segundo Sá, Machado e Almeida (2019), no artigo *O encontro da Guerra Cibernética com as Guerras Eletrónica e Cinética no âmbito do Poder Marítimo*, publicado na Revista Escola de Guerra Naval na edição de janeiro/abril 2019, são de seguida apresentados alguns exemplos de atos de Guerra Cibernética ocorridos nos últimos anos.

"[…]

ATOS DE GUERRA CIBERNÉTICA

Até o presente, a humanidade não experimentou a guerra cibernética de forma tão ampla quanto o fez com a guerra cinética. Se, por um lado, os conhecimentos sobre a guerra cinética foram construídos com base em observações e registros feitos ao longo de milhares de anos, por outro, os conceitos sobre a guerra cibernética se baseiam em experiências adquiridas ao longo de algumas décadas. Ainda assim, os ataques cibernéticos já ocorridos representam uma valiosa fonte de informações para o estudo da guerra cibernética e suas vertentes. Esta seção, apresenta exemplos de ataques de guerra cibernética com diferentes propósitos e formas de emprego. Embora, os ataques aqui descritos não tenham sido praticados em áreas navais, isto é, contra belonaves, embarcações civis ou infraestruturas existentes nas margens, sob ou sobre a superfície da água, eles servem, de forma geral, como referência ou prova de conceito para possíveis ataques que possam vir a causar incidentes em jurisdições navais.

ATAQUE À ESTÔNIA

Em 2007, a Estônia foi alvo de uma série de ataques cibernéticos que afetaram de forma significativa serviços essenciais do país. Para compreender a motivação dos ataques é necessário retornar ao final da Segunda Guerra Mundial. Com a Grande Guerra Patriótica[13], o Exército Vermelho tirou a Estônia do domínio nazista, forçando a sua integração à União das Repúblicas Socialistas Soviéticas (URSS). Com a desintegração da URSS, a Estônia torna-se independente e estabeleceu novamente a sua capital em Tallin. Durante o seu domínio, para que os povos do leste europeu se lembrassem dos sacrifícios feitos para libertá-los dos nazistas, a URSS ergueu grandes estátuas de um heroico soldado do Exército Vermelho, em muitas capitais da região, assim como fez em Tallin.

Tais estátuas eram vistas com muito apreço pelos líderes soviéticos. No entanto, aos olhos dos estonianos, a estátua erguida em Tallin representava um símbolo das cinco décadas de opressão que eles foram obrigados a passar como parte da URSS (CLARK; KNAKE, 2010). Assim, em 2007, atendendo aos sentimentos da população, o legislativo da Estônia aprovou a Lei das Estruturas Proibidas que determinava a remoção da estátua do soldado do Exército Vermelho, o que desagradou Moscou. Para evitar um incidente, o então presidente da Estônia vetou a lei. Nesse contexto, as pressões em torno da preservação, ou não, do símbolo soviético aumentaram.

De um lado, a opinião pública estoniana defendia a remoção da estátua e um grupo nacionalista a tentava destruir. De outro, grupos étnicos russos dedicados a protegê-la se tornavam cada vez mais ativos. Conflito culminou em uma revolta, conhecida como a Noite de Bronze (KAISER, 2015), que se seguiu da remoção da estátua para um cemitério militar. Foi quando o conflito migrou para o ciberespaço. A Estônia foi atingida por um ataque DDoS[14] de grande escala – até então o maior registrado. O ataque, lançado por diversas botnets[15], durou semanas e derrubou serviços eletrônicos do governo, bancos, sites de jornais e servidores da rede de telefonia. Devido ao grande impacto, o País Báltico levou o caso ao Conselho do Atlântico Norte, da OTAN. A Estônia alegou que os computadores que controlavam as botnets estavam na Rússia que, por sua vez, negou estar envolvida nos ataques cibernéticos (CLARK; KNAKE, 2010).

GUERRA RUSSO-GEORGIANA

Outro ataque cibernético conhecido – também envolvendo uma antiga república soviética – ocorreu em 2008 na Geórgia (SHAKARIAN, 2011), durante a chamada Guerra Russo-Georgiana. Na época, a Ossétia do

[13] Termo usado pelos russos para se referir à Segunda Guerra Mundial.

[14] No contexto dos serviços de internet, um ataque de negação de serviço, ou *Denial of Service* (DoS), é um tipo de ataque em que o serviço executado por um determinado servidor é interrompido devido à quantidade de requisições maior do que a sua capacidade de processamento e resposta. Um ataque distribuído de negação de serviços, ou *Distributed Denial of Service* (DDoS), por sua vez, é um ataque DoS em que um grande conjunto de equipamentos – composto por até milhares de máquinas – é usado para gerar o tráfego responsável por sobrecarregar o servidor e negar o seu serviço. Os equipamentos atacantes, denominados *zumbis*, podem ser computadores, servidores, equipamentos de rede ou mesmo dispositivos de *Internet* das Coisas, ou *Internet of Things* (IoT).

[15] Rede de dispositivos *zumbis*, ou bots, controlados remotamente por um computador mestre que, por sua vez comanda os ataques DDoS.

Sul era reconhecida internacionalmente como território da Geórgia, no entanto se considerava independente e recebia proteção, financiamento e vivia sob influência russa (CLARK; KNAKE, 2010). Naquele ano, rebeldes da Ossétia do Sul organizaram uma série de ataques com mísseis contra aldeias da Geórgia. Em resposta, a Geórgia bombardeou a capital da Ossétia do Sul e invadiu a região. No dia seguinte à invasão georgiana, veio a resposta do exército russo expulsando os militares georgianos da Ossétia do Sul. Ocorre que a ofensiva física não foi a única deflagrada contra a Geórgia.

Antes que os ataques cinéticos começassem, ataques cibernéticos já atingiam sites do governo georgiano. Ao longo do conflito, a Geórgia sofreu ataques DDoS direcionados aos seus meios de comunicação, com o objetivo de dificultar que os georgianos percebessem o que estava acontecendo. Os sistemas bancários, de cartões de crédito e de telefonia móvel foram afetados. A maioria dos roteadores que conectavam a Geórgia à Internet, via Turquia e Rússia, foram atacados. A Geórgia perdeu o acesso às fontes de informação e notícia externas. No auge da ofensiva, seis botnets foram mobilizadas para gerar o tráfego de ataque (CLARK; KNAKE, 2010). Embora alguns especialistas considerem que a coordenação entre os ataques cibernéticos e cinéticos tenha sido baixa (SHAKARIAN, 2011), e os russos alegarem que os ataques cibernéticos estavam fora do comando do Kremlin (CLARK; KNAKE, 2010), alguns eventos identificados sugerem ter havido tal coordenação. As instalações físicas da mídia e de sistemas de comunicação, por exemplo, não sofreram ataques cinéticos, apenas cibernéticos. Além disso, hackers russos atacaram um site usado para aluguel de geradores elétricos a diesel, provavelmente em complemento aos ataques convencionais que atingiram a infraestrutura elétrica do país (SHAKARIAN, 2011). É digno de nota que, segundo Shakarian (2011), os objetivos de isolar e desgastar a Geórgia foram limitados em seu escopo, tendo os atacantes evitado causar danos permanentes às redes georgianas e aos seus sistemas SCADA[16].

STUXNET

O ataque a sistemas SCADA, com consequências cinéticas diretas no mundo real, é verificado em um contexto diferente da Guerra Russo-Georgiana, com o emprego da – possivelmente – mais emblemática arma cibernética já usada: o *malware Stuxnet*. Seu propósito estratégico não foi a negação de serviços de internet, mas sim a negação de armas nucleares ao Irã de forma furtiva e sem o emprego de armas físicas. Mais especificamente, seu alvo eram as centrífugas de enriquecimento de urânio que operavam na usina de Natanz. Tais centrífugas, que funcionavam em um sistema de cascatas, eram controladas e operadas por meio de um sistema SCADA composto por controladores Siemens STEP 7.

Utilizando a analogia feita em (ZETTER, 2014), podemos descrever o Stuxnet como um míssil digital usado para transportar dois tipos de ogiva. A porção "míssil" se encarregava de transportar as ogivas digitais até os Controladores Lógicos Programáveis (CLP) que controlavam as centrífugas. Em outras palavras, a parte "míssil", era responsável por fazer com que o *malware* – mais especificamente um *worm* – se propagasse e replicasse até encontrar um sistema que tivesse a assinatura do sistema a ser atacado. Uma vez encontrando o sistema alvo – CPLs Siemens conectados às centrífugas –, o *worm* liberava as ogivas digitais que se instalavam nos CLPs e iniciavam ações sutis de degradação e destruição das centrífugas. Uma das ogivas digitais continha um código que alterava a velocidade de rotação das centrífugas de forma a reduzir a eficiência do processo de enriquecimento, causando também vibrações destrutivas. A outra ogiva atuava na abertura e fechamento das válvulas que interconectavam as centrífugas em cascata, causando aumento de pressão interna e avaria das centrífugas. Cabe ressaltar que o sistema de controle das centrífugas do Irã não estava diretamente conectado à Internet, de forma que, para alcançar a rede de controle, o *malware* precisava vencer o *air gap*[17] existente entre as duas redes. Sendo assim, dentre outras formas de difusão, o *Stuxnet* se propagava através de mídias removíveis (*pen drives*) e instalava seu código malicioso nos CLPs através das máquinas que eram utilizadas para programá-los.

Após a descoberta do *Stuxnet*, pesquisas demonstraram que, ele além de complexo, dispunha de uma quantidade de recursos nunca antes vistos juntos em uma arma digital. Em sua parte "míssil", o *malware* reunia ao todo oito formas de propagação (ZETTER, 2014), das quais quatro eram *zero-day exlpoits*[18] (FALLIERE, 2011), o que demonstra o grau de comprometimento e investimento aplicado no projeto. O *Stuxnet* foi

[16] Os sistemas de Supervisão e Aquisição de Dados, ou *Supervisory Control and Data Acquisition* (SCADA), são sistemas usados para controlar, monitorar e fazer a aquisição de dados de sistemas físicos automatizados. Os sistemas físicos controlados vão desde plantas industriais até infraestruturas críticas.

[17] Air gap é o termo utilizado para se referir à medida de segurança de redes onde a rede a ser protegida é fisicamente isolada das redes inseguras – como a Internet, por exemplo –, não havendo conectividade entre elas.

[18] Zero-day exploits são ferramentas que exploram vulnerabilidades do tipo zero-day – i.e. vulnerabilidades desconhecidas por quem estaria interessado em mitigá-las. Vulnerabilidades zero-day são raras e seus exploits, quando comercializadas no mercado cinza ou negro (ZETTER, 2014) de armas digitais, são caros.

encontrado em 2010 e investigado por diversos especialistas ao redor do mundo (ZETTER, 2014), tanto da área de sistemas de controle industriais (LANGNER, 2011), quanto da área de segurança da informação (FALLIERE, 2011). As evidências e investigações apontam para a autoria conjunta de EUA e Israel (ZETTER, 2014). O *Stuxnet* é considerado uma prova de conceito de como as armas digitais podem afetar diretamente o mundo físico, sendo capazes de cumprir os mesmos propósitos estratégicos de ataques com armas cinéticas como mísseis e bombas.

ATAQUE AO GASODUTO TRANSIBERIANO

Embora o *Stuxnet* seja considerado um marco nos ataques a sistemas ciberfísicos, a literatura (WEISS, 1996; CLARK; KNAKE, 2010; MILLER, 2012) indica a existência de outra bomba lógica de impacto físico anterior ao referido *worm*. A arma teria sido usada para causar destruição em uma tubulação de transporte de gás situada na Sibéria, no início da década de 1980 (CLARK; KNAKE, 2010) – ou seja, antes mesmo de a Internet estar difundida como nos dias do *Stuxnet*. À época, sem a grande conectividade da rede mundial de computadores, os atacantes – isto é a CIA com o apoio de Canadenses, segundo (CLARK; KNAKE, 2010) – utilizaram outra estratégia para fazer o código malicioso chegar ao sistema de controle do gasoduto. Para tal, implantaram o código malicioso diretamente no controlador, antes mesmo de o equipamento ser obtido pela Rússia e instalado em seu sistema de automação de dutos (CLARK; KNAKE, 2010).

O controlador seria utilizado para comandar a abertura e o fechamento de válvulas, bem como para controlar o acionamento de bombas que faziam fluir gás na tubulação. Sendo assim, segundo (CLARK; KNAKE, 2010), o código malicioso foi programado para comandar o fechamento da válvula de um segmento do gasoduto, ao mesmo tempo em que a bomba era acionada em capacidade máxima para injetar gás dentro da tubulação. O acionamento indevido dos atuadores do sistema – i.e. a bomba e a válvula – resultou no aumento da pressão interna do duto, causado, por sua vez, a maior explosão não nuclear até então registrada, acima de três quilotons (CLARK; KNAKE, 2010; MILLER, 2012).

OPERAÇÃO ORCHARD

Um novo tipo de ataque veio à discussão com a Operação ORCHARD, lançada em 2007 pelo Estado de Israel contra a Síria. Na madrugada de 06 de setembro de 2007, aeronaves da Força Aérea Israelense entraram no espaço aéreo sírio e bombardearam uma instalação industrial que estava sendo construída no território daquele país. Tal instalação era uma planta nuclear que, segundo Clark e Knake (2010), a Síria estava construindo com o apoio da Coreia do Norte. Na ocasião, além da repercussão do próprio bombardeio e das discussões em torno do propósito da planta atacada, chamou a atenção internacional o fato de a Síria, que já havia investido bilhões de dólares em sistemas de defesa aérea (CLARK; KNAKE, 2010), não ter reagido ao ataque. Naquela noite, a Síria estava em alerta, uma vez que Israel, na manhã anterior, havia posicionado suas tropas nas colinas de Golã. Os militares sírios observavam atentamente seus radares. No entanto, no momento em que as aeronaves F-15 Eagles e F-16 Falcons de Israel invadiram o espaço aéreo sírio, nada de incomum apareceu nas telas dos radares do sistema de vigilância.

Na busca por explicações plausíveis, para a falha do sistema de vigilância sírio, alguns analistas sugerem que aquele país tenha sido vítima de um ataque de guerra eletrônica. No entanto, o ataque se diferenciava das demais Medidas de Ataque Eletrônico[19] (MAE) conhecidas, por explorar uma vulnerabilidade implantada no domínio cibernético do sistema de vigilância sírio (ADEE, 2008; CLARK; KNAKE, 2010).

Radares, como sensores, são interfaces abertas para o ambiente. Para captar informações sobre possíveis alvos, um radar transmite pulsos por meio de sua antena e capturam, de uma forma geral, todo e qualquer eco que chegue de volta ao seu recetor. Os ecos recebidos, por sua vez, são digitalizados, armazenados em uma memória e processados por um sistema computacional que apresenta ao operador informações relevantes sobre os alvos detetados como, por exemplo, posições e velocidades (BOLE, 2005). Dessa forma, é possível afirmar que um transmissor, apto a transmitir pulsos no mesmo padrão dos transmitidos pelo radar, seja capaz de fazer com que ecos falsos – sinteticamente produzidos – cheguem à antena do radar (ABDALLA et al., NENG-JING; YI-TING, 1995). Estes ecos falsos, uma vez digitalizados, passam a ser representados na forma de bits na memória do radar (BOLE; DINEY; WALL, 2005). Isto significa dizer que é possível manipular os bits da memória de dados de um radar por meio de MAE conhecidas – o que não representa grande novidade em face do estado da arte da GE (ABDALLA et al.; 2015). No entanto, neste ataque, é possível que houvesse no sistema de vigilância um gatilho digital – isto é uma vulnerabilidade implantada em *software* e/ou *hardware* –

[19] De acordo com (MARINHA DO BRASIL, 2014), as MAE correspondem a um "conjunto de ações tomadas para evitar ou reduzir o uso efetivo, por parte do inimigo, do espectro eletromagnético e, também, degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro". As MAE têm natureza fundamentalmente tática e representam um dos três ramos das Medidas de Guerra Eletrônica (MGE) – que também englobam as Medidas de Proteção Eletrônica (MPE) e as Medidas de Apoio à Guerra Eletrônica (MAGE) (MARINHA DO BRASIL, 2014).

observando constantemente as informações captadas e salvas na memória do radar, em busca de informações com um padrão específico que acionasse tal gatilho digital (ADEE, 2008; CLARK; KNAKE, 2010). Tal gatilho digital, por sua vez, iniciaria rotinas maliciosas no sistema computacional dos radares. Basicamente seriam duas rotinas maliciosas: uma rotina de gravação e outra de reprodução de cenários. As informações, ou bits, com tal padrão específico de acionamento seriam introduzidas na memória pela MAE, por meio da antena do próprio radar. Uma vez identificado o padrão de acionamento da rotina de gravação, o gatilho digital dava início a gravação de um cenário a priori normal – i.e. sem alvos que representassem ameaças. Posteriormente, ao identificar o padrão de acionamento da rotina de reprodução, o gatilho digital passava a reproduzir para os operadores o cenário de operação normal, previamente gravado durante a rotina de gravação. Dessa forma, estima-se que uma MAE em conjunto com um gatilho digital no sistema computacional do radar tenha sido capaz de negar aos operadores sírios a deteção de aeronaves inimigas durante a execução do bombardeio (CLARK; KNAKE, 2010).

SÍNTESE DOS ATAQUES

As ações de guerra cibernética apresentadas nesta seção não esgotam os ataques cibernéticos já ocorridos. No entanto, demonstram a diversidade dos ataques, bem como as formas em que eles foram eficazmente usados como ferramenta para causar danos físicos ou econômicos a nações adversárias, ou mesmo para apoiar a execução de ataques cinéticos em operações militares. No caso do ataque à Estônia, notamos que os ataques executados foram exclusivamente cibernéticos, causando impacto no mundo real por meio da negação de serviços essenciais para a economia e sociedade estonianas. Na guerra Russo-Georgiana, os ataques cibernéticos foram empregados para apoiar ataques de forças convencionais (SHAKARIAN, 2011), com algum grau de coordenação entre eles. Nos exemplos do *Stuxnet* e do ataque ao gasoduto transiberiano, as armas digitais foram empregadas para causar danos físicos diretos ao inimigo, sem a necessidade do uso de forças convencionais. Já na operação ORCHARD um ataque envolvendo ações de guerra cibernética e eletrônica foi usado para apoiar, de forma coordenada, a execução de ataques usando forças convencionais. É possível, portanto, perceber nesses exemplos três tipos de ataque:

- Ataques cibernéticos com o objetivo de afetar sistemas de informação e de comunicação, porém sem o propósito de afetar diretamente sistemas físicos (ataques à Estônia e da Guerra Russo-Georgiana);
- Ataques cibernéticos com o propósito de afetar diretamente sistemas físicos (*Stuxnet* e o ataque ao gasoduto transiberiano); e
- Ataques cibernéticos envolvendo MAE visando prejudicar a obtenção de informações táticas, mas sem o propósito de manipular diretamente sistemas físicos (ataque na Operação ORCHARD).

Uma análise mais profunda dessas ofensivas sugere a possibilidade de serem desenvolvidos ataques cibernéticos envolvendo MAE, capazes de afetar diretamente sistemas físicos. Em sistemas navais, mais especificamente, tal possibilidade decorre da crescente integração entre sistemas computacionais, plantas físicas, sistemas de comunicação e sensores que fazem uso do espectro eletromagnético (BOYES; ISBELL, 2017; LAGOUVARDOU, 2018; BHATTI; HUMPHREYS, 2017). Desse modo, o foco da discussão deste trabalho se concentra em ações ofensivas que transitam entre os domínios cibernético, eletrônico e cinético, com possíveis impactos no ambiente naval […]" (Sá, Machado, & Almeida, 2019, pp. 93-100).

Anexo B — *CD-Deploy overview*

Quadro 5 – Descrição da capacidade de CD-Deploy

Code	*CD-DEPLOY*
Full Name	*Deployable Cyber Defence*
Capstone Statement	
1.01	*Capable of independently applying security measures in deployed networks for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication, and non-repudiation.*
Principal Statements	
2.01	*Capable of organizing and operating security measures used for CIS in a way that prevents attacks and faults from happening and/or mitigates their impact, by implementing: boundary protection; endpoint protection; network protection; physical and personnel protection; deception solutions.*
2.02	*Capable of organising and operating security measures used to protect data in a way that helps prevent data compromise and/or mitigates its impact by implementing: security metadata management; information redaction/sanitization; secure information deleting; assignment and binding of CIS security markings and labels.*
2.03	*Capable of supporting data confidentiality, integrity and availability through the use of modular, reprogrammable, interoperable, backwards compatible and releasable (to both non-NATO partners and partners of opportunity) cryptography.*
2.04	*Capable of maintaining assured security robustness through cryptographic effectiveness and efficiency based on use of latest technology advances, regular updates, integration with Service Management and Control (SM&C) and interoperability testing and assessment capabilities.*
2.05	*Capable of planning and controlling attributes related to entities and access to CIS services and information, by implementing: 1) identity management (planning identity management, controlling credentials and identities, authentication); 2) Access management (managing access policy, enforce and authorize access).*
2.06	*Capable of planning and controlling the CIS assets, CIS services, and their configuration by: 1) managing asset inventory; 2) CIS configuration and update management; 3) cryptographic equipment management; 4) effective and efficient federated key management and distribution, including non-NATO partners; 5) service level agreement management.*
2.07	*Capable of collecting sensor data about all ongoing activities as well as the state of all relevant CIS components in a comprehensive fashion through the use of sensors and the alignment of syntax, reference points, and semantics for that sensor data.*
2.08	*Capable of detecting malicious activity and faults by analysing sensor data in order to identify malicious and suspicious actions and activities, and determine the meaning and importance of these activities by looking at their local and a global impact by 1) identifying actions (finding, listing and characterizing related sensor data and recognizing actions); 2) identifying activities (finding, listing and characterizing related actions and recognize activities); 3) estimating activities and context.*
2.09	*Capable of reacting to incidents in order to stop and mitigate their effect in a timely manner by 1) incident management; 2) Decision making process (identifying options, impact, stakeholders, decision makers and coordinating/disseminating decisions; 3) external response coordination; 4) preserve chain of evidence.*
2.10	*Capable of recovering from a compromise in the CIS's security resulting from an attack or fault by restoring the system and information integrity, the system availability, and the registration of any compromised information by 1) assessing damage and attacks/faults (including malware and failed software assessment); 2) restoring system*

	and information integrity; 3) restoring service availability; 4) registering compromised information.
2.11	*Capable of planning risk management; assessing the risk based on analysed threats, values, dependencies, and asset attributes; accrediting through verification of policy compliance and validation of the risk management; planning business continuity; managing the treatment of risk; and communicating the risk to the relevant stakeholders.*
2.12	*Capable of planning and controlling the trust that can be put in CIS components through the planning of how to manage trustworthiness, the assessment of CIS components and other parties, and the management of trustworthiness treatment and supply chain security.*
2.13	*Capable of analysing and evaluating the historical and actual effectiveness of CIS Security, as well as the efficiency with which CIS Security is provided.*
2.14	*Capable of systematically reviewing the way in which a CIS has been operated, including how risk has been managed, in order to help achieve accountability.*
2.15	*Capable of managing CIS Security requirements, designing CIS Security (by adopting or developing CIS Security models/architectures/designs to design adaptable and resilient CIS), implementing CIS Security (by maintaining secure software, cryptographic CIS Security components and services, and integrating CIS Security components), verifying and validating CIS Security to ensure that the implemented CIS is built in an efficient and adaptive manner, meets the security requirements, functions correctly, and is aligned with high-level security direction and guidance.*
2.16	*Capable of determining what information is needed for CIS Security, who needs it, and how it will be collected, assessed, and exploited.*
2.17	*Capable of gathering and receiving CIS Security information from various sources, in particular information about malicious and non-malicious threats and regarding the value of CIS assets, CISs as a whole, and the missions they support.*
2.18	*Capable of analysing and evaluating collected CIS Security information.*
2.19	*Capable of ensuring that available CIS Security information is optimally utilized to support CIS Security, through reporting and disseminating it as required in support of other CIS Security capabilities as well as to relevant partners.*
2.20	*Capable of deploying a modular and scalable CD module that can be adapted to the full range of deployable CIS in terms of size, complexity, and geographic distribution.*
2.21	*Capable of creating a recognised cyber operations picture in a localised time and space to provide commanders with enhanced situational awareness, improved understanding, decision support and enables better delivery of cyber effects.*
Enabling Statements	
3.01	*Capable of deploying in theatre for operations that cover the entire spectrum of Alliance missions, including high intensity combat operations, and in any environmental conditions.*
3.02	*Capable of integrating into a deployed CIS Unit.*
3.03	*Capable of independent team response deployment to provide support to the subordinate units of the supported headquarters in the event of cyber incidents.*
3.04	*Capable of operating only as part of a larger unit or on an installation from which it may draw logistic support and force protection.*
3.05	*Capable, on request, of providing support to the protection of critical civilian infrastructure.*

Fonte: Disponível a partir da *NATO Communications and Informations* (NCI) *Agency* (2016, p. 4 e 5)

Anexo C — Requisitos estabelecidos pela OTAN para a componente de GE

Tendo por referência os requisitos definidos pela OTAN, *NATO's Minimum Capability Requirements Parts II - Dec2011*, a CompGE deverá estar capacitada para:

- Efetuar a interceção, recolha, processamento, geolocalização e exploração de emissões de Sistemas de Comunicações através da rádio frequência (Radio Frequency-RF) e Não-Comunicações (essencialmente radares), para gerar Eletronic Support Measures (ESM) e SIGINT. Deste último, as Comunications Intelligence (COMINT) e Eletronic Intelligence (ELINT) e conduzir atividades de Empastelamento e Deceção sobre os sistemas de Comunicações e Não-Comunicações das forças opositoras;

- Efetuar a interceção, recolha e processamento, de emissões de Sistemas de Comunicações e Não-Comunicações (incluindo engenhos explosivos improvisados ativados por controlo remoto – Remote Controlled Improvised Explosive Devices (RC IED)), na sua área de operações;

- Efetuar ações de pesquisa e radiolocalização de emissões rádio de Sistemas de Comunicações (HF, VHF e UHF) e de Sistemas de Não-Comunicações (essencialmente radares);

- Reconhecer e identificar emissores através das suas caraterísticas de emissão específicas, comparando com uma base de dados de Electronic Order-Of-Battle (EORBAT);

- Difundir informação em tempo oportuno e de modo seguro;

- Realizar atividades de Empastelamento, Deceção e Neutralização sobre os sistemas de Comunicações (HF/VHF/UHF) e Não - Comunicações das forças opositoras;

- Recorrer a Medidas de Proteção Eletrónica para a sobrevivência dos Sistemas da Guerra Eletrónica e das forças em geral;

- Ser empregue em apoio às unidades de manobra e na proteção da força;

- Contribuir para o ISTAR;

- Integrar o sistema JISR;

- Atuar por um período de 3 dias sem ser apoiada ou reabastecida;

- Garantir um nível de proteção adequado contra Engenhos Explosivos Improvisados (Improvised Explosive Devices - IED), de acordo com STANAG 2294 C-IED (Edition1) Counter Improvised Explosive Device (CIED) Training Standard;

- Garantir proteção Nuclear, Biológica, Química e Radiológica (NBQR) adequada a todo o pessoal e equipamento orgânico.

Anexo D — *Cyber Warfare* segundo Marcelo Rios

O presente Anexo apresenta duas transcrições de dois videos do autor do canal *Hoje no Mundo Militar*, Marcelo Rios, investigador nas áreas de história militar, particularmente na vertente militar. Autor, criador e administrador de dois canis de *Youtube* onde apresenta grande parte do seu tabalho: (i) *Hoje na Segunda Guerra Mundial*, com 518 mil subscritores; e (ii) *Hoje no Mundo Militar*, com 1,43 milhões de subscritores. Enfatiza, que é um trabalho bastante grande de toda a equipa, tanto na edição como na pesquisa que se materializa nos videos apresentados, e que para os temas é feita uma pesquisa, o mais profissional possivel e suportada em fontes seguras e confiáveis.

Cyber Warfare, porque um hacker pode ser mais perigoso do que uma bomba atômica!

Transcrição de um vídeo disponível no *Youtube* (Rios, 2018)

"[…] Imagine que um dia de manhã você acorda é descobre que a sua cidade não tem energia elétrica, você corre para o trabalho mas descobre que o metrô está fechado devido a avarias técnicas estranhas, você entra num caixa automático para levantar dinheiro para pegar um táxi e descobre que a sua conta corrente está inacessivel, escuta através de um velho rádio a pilhas que pertencia ao seu pai que todos os serviços online estão desligados que o serviço nacional de fornecimento de eletricidade foi desativado, que todas as comunicações telefônicas e por satélite não funcionam, que a rede de água potável e de tratamento de esgotos da cidade está um caos, que as informações bancárias de todas as empresas e de todos os cidadãos foram roubadas ou apagadas.

Na calada da noite sem aviões sobrevoando os céus sem exclusões provocadas por bombas ou mísseis e sem soldados inimigos invadindo as cidades, o seu país foi arremessado aos pontapés de volta para a idade da pedra, ficando completamente à mercê dos seus inimigos. Você não sabe que provavelmente nunca saberá mas o seu país acabou de ser destruído por um grupo de jovens a maioria deles ainda vivendo com os pais. Essa cena apocalíptica parece ter saído de um filme de ficção científica mas isso pode acontecer a qualquer momento e em qualquer país do mundo. Há um termo genérico que serve para identificar ataques desse tipo *Cyber Warfare*, mas a definição completa de *Cyber Warfare* é mais abrangente, inclui também a espionagem o roubo discreto de informações importantes sigilosas e a sabotagem de Infraestruturas, como os sistemas de fornecimento de energia elétrica e de redes de computadores, que podem ser do governo, dos militares ou de instituições privadas como os bancos. Esses atos podem ser organizados por nações rivais, por empresas concorrentes, por grupos terroristas ou por indivíduos criminosos à procura de lucro fácil. Mas não há dúvidas de que os grupos mais bem preparados para esse tipo de ação são aqueles financiados por estados. Alguns países como a China, a Rússia, os Estados Unidos e o Reino Unido, têm orçamentos multimilionários dedicados especificamente para essa área, através dessas unidades esses governos criam ferramentas e os meios para se defenderem de ataques ao mesmo tempo em que se capacitam também para o lado ofensivo dessa guerra. Outros países também muito bem posicionados nessa área são Israel, a Coreia do Norte e também o Irão.

Por exemplo em 2014 logo após a estreia do filme *A Entrevista*, que mostrava uma entrevista fictícia ao ditador norte coreano Kim Jong-un, a *Sony Pictures* o estúdio responsável pelo filme, foi alvo de uma série de ataques cibernéticos com as investigações do FBI levando a um conhecido grupo de hackers norte coreanos, financiados pelo governo de Pyongyang. Em 2015 o governo alemão posicionou-se oficialmente ao lado da Ucrânia na questão da Crimeia e dos separatistas no leste daquele país e nesse mesmo ano os computadores do parlamento alemão foram ferozmente atacados, resultando em mais de 20000 computadores bloqueados e infectados com vírus. As investigações conduziram a um grupo de hackers russos que no ano anterior já tinha um atacado os computadores do sistema eleitoral ucraniano. Em dezembro de 2016 em pleno inverno mais de duzentos mil ucranianos ficaram sem energia elétrica durante várias horas, como resultado de um ataque cibernético contra três centrais elétricas ucranianas. Essas centrais precisaram de meses até se recuperarem completamente do ataque, cuja origem acredita-se estar na Rússia. Durante muitos anos os chineses conseguiram entrar em redes de computadores de grandes empresas americanas como a *Boeing* e a *Lookheed*, roubando muitos projetos que hoje são utilizados em produtos, veículos e aviões chineses.

Não há dúvidas de que as guerras já estão sendo travadas também no campo da internet, por exemplo no início de 2014 ao mesmo tempo em que tropas russas avançaram pela Crimeia, bloqueando os acessos por terra ao resto da Ucrânia, hackers atacavam os servidores ucranianos entupindo as máquinas com chamadas

falsas, num tipo de ataque conhecido como DoS[20]. Por conta desse ataque, o mundo só teve uma visão mais clara do que estava acontecendo na Crimeia, muitas horas depois do início do avanço russo.

O que aconteceu na Crimeia é o exemplo perfeito de como as guerras serão travadas no futuro, ao mesmo tempo em que os soldados avançam pelo terreno e os aviões cruzam os céus, um exército nas sombras avançará pelo mundo, bloqueando os sistemas cruciais impedindo a livre circulação de informações de. e para o campo de batalha. Proteger-se de ataques assim é extremamente difícil, como referi, as grandes potências investem orçamentos multimilionários que também são utilizados para a defesa, contra ataques desse tipo. Mas nós [estados com menos meios], meros indivíduos não contamos com muitos recursos além daquelas práticas saudáveis como por exemplo, não executar programas recebidos por e-mail mesmo que tenham sido enviados por amigos e familiares, não clicar em links suspeitos e manter sempre o antivírus ativado em devidamente atualizado. É o mínimo que podemos fazer para nós protegermos nesse novo campo de batalha do século XXI […]" (Rios, 2018).

Guerra Cibernética, o novo campo de batalha do século 21

Transcrição de um vídeo disponível no *Youtube*, do canal *Hoje no Mundo Militar*. (Rios, 2016).

"[…] Não é de hoje que a informação e a capacidade de conhecer as intenções do inimigo são essenciais para a vitória no campo de batalha. Durante a Segunda Guerra Mundial os aliados, graças ao incrível trabalho de desencriptação executado pelos britânicos, liderados pelo matemático equipe do analista Alan Turing, eram capazes de ler as ordens enviadas pelos alemães através da sua máquina *enigma*, um equipamento que em que encripttava as mensagens em milhões de combinações possíveis. Graças a esse esforço muitos dos movimentos dos alemães no campo de batalha eram previamente conhecidos, o que facilitou muito a vitória dos aliados na guerra.

O contrário também provou ser tremendamente vantajoso ou seja, fazer o inimigo pensar uma coisa quando o que se planejava era outra coisa completamente diferente. Por exemplo, graças a uma série de informações cirurgicamente plantadas, os aliados conseguiram fazer os alemães acreditarem que o desembarque na França de 1944, ocorreria em Pas-de-Calais, na região francesa a apenas 35 km da costa inglesa, quando na verdade o plano aliado envolvia o desembarque de dezenas de milhares de soldados na Normandia, muito mais ao sul. Graças a essa manobra de contra informação os aliados encontraram muito menos resistência na Normandia, o que facilitou bastante o trabalho dos soldados no campo de batalha.

E hoje em dia na era da internet, da informação instantânea, essa estratégia evoluiu ao nível nunca antes visto. Se antigamente era necessário contratar espiões para executarem missões perigosas que incluíam a invasão de instalações inimigas, nos tempos atuais com informações valiosas e sensíveis armazenadas em computadores ligados à internet, qualquer jovem com os equipamentos e os meios adequados, é capaz de ter acesso a essas informações. Como é óbvio há diversos métodos e formas de proteger informações militares valiosas, alguns mais eficientes do que outros, mas de forma geral a partir do momento em que um servidor está ligado de alguma forma internet, o risco de ser invadido infectado é real. O termo guerra cibernética é relativamente novo e pode ser definido como ações tomadas por uma nação com o objetivo de invadir os computadores de outra nação, com o propósito de roubar informações, destruir sistemas, ou causar o mau funcionamento de instalações. Trata-se de uma atividade tão importante que todas as principais potências militares do mundo já criaram unidades e agências especiais dedicadas a guerra cibernética.

A guerra cibernética envolve basicamente 2 tipos de atividade: a espionagem é sabotagem, que pode envolver desde a destruição de projetos, planos de documentos, até ações diretas contra Infraestruturas controladas por computadores, como o sistema de distribuição de eletricidade, centrais nucleares, sistemas de transporte, estações de tratamento de água, entre outros.

Através da guerra cibernética países relativamente pequenos podem se destacar e alcançar vantagens sobre as grandes potencias militares, motivo pelo qual países como Irão e a Coreia do Norte, supostamente investem tanto nesse tipo de atividade. Mas como é óbvio, países como a China, a Rússia e os Estados Unidos são os que mais se dedicam a guerra cibernética. Não se sabe exatamente quando os recursos cada país dedica especificamente para essa área mas acredita-se que seja valores bem elevados que crescem de ano para ano.

A espionagem é a face mais visível entre aspas, da guerra cibernética com países como os Estados Unidos, investindo pesado na interceptação de mensagens alheias, com destaque para as escutas telefônicas que os norte-americanos fizeram de líderes estrangeiros como Ângela American, e a própria ex-presidente brasileira Dilma Rousseff, que teve o seu telefone supostamente grampeando.

[20] *Denial of Service*.

Os chineses também não ficam atrás na guerra cibernética, principalmente através da invasão de sistemas informáticos. De acordo com reportagem de artigos referindo relatos de desertores chineses, a China tem neste momento milhares de espiões que trabalham com engenheiros em grandes empresas de informática dos Estados Unidos, e na Europa. Através dessa intrincada rede os chineses conseguem ter acesso a informações que de outra forma seria praticamente impossível. A Índia, que é semelhança da China forma milhares de novos engenheiros altamente qualificados todos os anos, também tem investido pesado nesse campo.

É prática comum de muitos governos oferecerem oportunidades de emprego hackers apanhados cometendo crimes cibernéticos, já que são indivíduos com uma clara aptidão para esse tipo de atividade.

Assim como a guerra biológica é envolve a criação de doenças destinadas a matar o inimigo, a guerra cibernética envolve também a criação de vírus especialmente criados para atacar e destruir determinados alvos. Por exemplo em setembro de 2010 um centro iraniano de enriquecimento de urânio foi atacado por um vírus obrigando a paralisação temporária das atividades. Em 2008 quando a Rússia invadiu a Geórgia, um pequeno país às margens do mar Negro, sites e instituições georgianas foram atacadas por hackers supostamente russos, afetando diversos sistemas do país. Em 2013 Edward Snowden, na época funcionário da CIA, copiou uma série de informações sensíveis referentes a programas norte-americanos de espionagem. Essas informações foram divulgadas na internet e indicavam a existência de uma gigantesca rede global de espionagem, montada pelos Estados Unidos, na qual boa parte das trocas de mensagens, telefonemas e e-mails, são interceptados e lidos por agências governamentais norte-americanas. Snowden foi acusado de espionagem alta traição, tendo-se refugiado na Rússia em junho de 2013.

O mundo cibernético será sem dúvida um campo de batalha cada vez mais importantes no futuro e a guerra cibernética ditará o resultado das batalhas travadas entre países […]" (Rios, 2016).

Anexo E — STUXNET – *Anatomy of a computer virus*

De seguida é apresentado um texto, transcrito de uma aula do curso ADL 076 *Cyber defence Awareness*, disponível na Plataforma da OTAN de e-learning, *Joint Advanced Distributed Learning* (JADL). Neste texto de 2011, é apresentada uma abordagem interessante, sobre o vírus STUXNET, identificando-o como sendo a primeira arma cibernética criada, e que se apresenta disponível em código aberto na internet.

"*In June last year a computer virus called Stuxnet was discovered lurking in the data banks at power plants traffic, control systems and factories around the world. Twenty times more complex than any previous virus code it had an array of capabilities, among them the ability to turn up the pressure inside nuclear reactors or switch off oil pipelines and Stuxnet could tell the system operators, everything was normal.*

Unlike most viruses, Stuxnet doesn't carry the usual forge security clearance that helps viruses burrow into systems, it actually had a real clearance stolen from one of the most reputable computer technology companies in the world.

It exploits security gaps this system creators are unaware of. These holes are known as zero days, and the most successful viruses exploit them. The details of a zero day can be sold on the black market for $100,000.

Stuxnet took advantage of 20 zero days, but once it got into a system it didn't always activate very deep in the Stuxnet code was a specific target without that target the virus remained dormant. What was he looking to shut down? The centrifuges that spin nuclear material at Iran's enrichment facilities.

Stuxnet was a weapon, the first to be made entirely out of code.

The Washington based Institute for science and International Security, says the virus may have shutdown 1000 centrifuges at Natanz, Iran's main enrichment facility last year. In November the International Atomic Energy Agency, UN Nuclear Watchdog, said Iran had suspended work at its nuclear facilities without explaining why. Many observers credited Stuxnet. Last month the Iranian government conceded the viruses infection of the Bashir nuclear facility still under construction, meant that switching the plant on it could lead to a national electricity blackout.

Iran has responded to the attack with an open call for hackers to join the Iranian Revolutionary Guard and has reportedly amassed the second largest online army in the world.

So, who was behind Stuxnet? There's no evidence beyond rumour. Some have it that Israel is responsible because the virus code apparently contains references to the Hebrew Bible. Others believe the US was involved in the testing and development. The finger has even been pointed at Siemens mobile phone company whose software is used by the Iranian regime.

The most important question may not be who designed it, but who will redesign it? The evolution has been so fast that nine months after its detection, the first virus could crash power grids or destroy oil pipelines, is available online for anyone to download and tinker with. You can watch people on YouTube pulling Stuxnet apart. It's an open source weapon, and there's no way of knowing who will use it, or what they will use it for." (JADL, 2011).

Apêndice A — Conceitos Fundamentais complementares

Quadro 6 – Conceitos Fundamentais complementares

Conceito	Definição	Fontes
Guerra Eletrónica *Electronic Warfare radioelektronnaya bor'ba*	*"[…] EW is military action that exploits EM energy to provide situational awareness and achieve offensive and defensive effects. EW, the conduct of EMO, is warfare in the EME. It comprises: Electronic Attack (EA) - use of EM energy for offensive purposes; Electronic Defence (ED) - use of EM energy to provide protection and to ensure effective friendly use of the EM spectrum; and Electronic Surveillance (ES) - use of EM energy to provide situational awareness and intelligence […]"*	*De acordo com doutrina OTAN* (NATO, 2015, p. 1.2)
	"[…] EW refers to any action involving the use of electromagnetic (EM) or directed energy to control the electromagnetic spectrum (EMS) or to attack the enemy. The purpose of EW is to deny the opponent an actual or perceived advantage in the EMS and ensure friendly unimpeded access to the electromagnetic environment […]"	De acordo com o Departamento do Exército dos EUA (US Army, 2007)
	"[…] is a type of armed struggle using electronic means against enemy C4ISR to "change the quality of information" or using electronic means against various assets to change the conditions of the operational environment. EW consists of suppression and protection […]"	*Voyennyy Entsiklopedicheskiy Slovar'* ("Military Encyclopedic Dictionary") (RUS)
Guerra Cibernética *Cyber Warfare*	"[…] Cyber war was defined as the systematic struggle in the cyber domain among states, political groups, and extremist and terrorist groups, where targets are information resources and whose properties (integrity, accessibility, and confidentiality) can be violated […]"	De acordo com o relatório (Lindsay, 2012, p. 21)
Ciberespaço *Cyberspace*	*"The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data."*	AJP-3.20 *Allied Joint Doctrine for Cyberspace Operations* (NATO, 2017 Draft, p. 4)
	"Ciberespaço consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação."	Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC, 2019, p. 2889)
Operação no Ciberespaço *Cybrespace Operation (CO)*	*"Actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders' objectives."*	AJP-3.20 *Allied Joint Doctrine for Cyberspace Operations* (NATO, 2017 Draft, p. 4)
	"Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). Cyberspace operations consist of three functions: offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations […]"	De acordo com o FM 3-38 (Headquarters, Department of the Army, 2014, pp. 1-3)

Conceito	Definição	Fontes
Operação no Ciberespaço Defensiva *Defensive Cybrespace Operation (DCO)*	*"Defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace."*	AJP-3.20 *Allied Joint Doctrine for Cyberspace Operations* (NATO, 2017 Draft, p. 4)
Operação no Ciberespaço Ofensiva *Offensive Cybrespace Operation (OCO)*	*"Actions in or through cyberspace that project power to create effects which achieve military objectives."*	AJP-3.20 *Allied Joint Doctrine for Cyberspace Operations* (NATO, 2017 Draft, p. 4)
Atividades Ciber Eletromagnéticas *CEMA*	*"[…] Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system (ADRP 3-0). CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO) […]"*	De acordo com o FM 3-38 (Headquarters, Department of the Army, 2014, pp. 1-1)
Ciberataques *Cyber attack*	"A cyberspace attack consists of actions that create various direct denial effects in cyberspace (for example, degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. For the Army, cyberspace attacks are a type of cyberspace operation employed primarily in support of OCO. Cyberspace attacks are primarily employed outside of LandWarNet, but they are coordinated and deconflicted inside of the Department of Defense information networks (DODIN)."	De acordo com o FM 3-38 (Headquarters, Department of the Army, 2014, pp. 3-3)
Ciberdefesa	"Ciberdefesa consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço. Por cibercrime entendem -se os factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa."	Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC, 2019, p. 2890)
Cibersegurança *Cyber Security (CS)*	*"The application of security measures for the protection of communication, information, and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation."*	AJP-3.20 *Allied Joint Doctrine for Cyberspace Operations* (NATO, 2017 Draft, p. 4)
	"Cibersegurança consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem."	Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC, 2019, p. 2889 e 2890)

Conceito	Definição	Fontes
xxx *Red Teams*	"*A red team is a team that is formed with the objective of subjecting an organisation's plans, programmes, ideas and assumptions to rigorous analysis and challenge. Red teaming is the work performed by the red team in identifying and assessing, inter alia, assumptions, alternative options, vulnerabilities, limitations and risks for that organisation. Red teaming is a tool set. Using it will provide the end user (commander, leader, or manager) with a more robust baseline for decision making*"	(UK Ministry of Defence, 2013, p. 9)
xxx *White Hackers*	"Esses são os hackers bonzinhos. São especialistas em segurança computacional que se concentram em fazer testes de penetração e outras metodologias de modo a garantir que os sistemas de informação de empresas são realmente seguros. Esses profissionais de segurança de TI usam um arsenal em constante evolução para enfrentar os hackers "ruins"."	Website de software de antivírus (McAfee, 2019)
xxx *Black Hackers*	"Esses são os hackers malvados, geralmente chamados simplesmente de hackers. O termo costuma ser usado especificamente para criminosos que invadem redes ou computadores, ou ainda que criam vírus de computador. Hackers do tipo Black Hat continuam a agir mais rapidamente do que os do tipo White Hat. Eles costumam encontrar o caminho que oferece menor resistência – seja erro humano ou negligência – ou criam um novo tipo de ataque. Puristas usam o termo "crackers" para se referir aos hackers do tipo Black Hat. A motivação desse tipo costuma ser vantagens monetárias."	Website de software de antivírus (McAfee, 2019)
xxx *Gray Hackers*	"Esses são hackers que não usam suas habilidades para benefício próprio, mas não operam de forma totalmente legal. Por exemplo, um hacker que invada o sistema de uma empresa para revelar uma vulnerabilidade e poste a descoberta na internet pode, em última instância, estar fazendo algo positivo para os clientes daquela empresa, mas, por outro lado, comprometeram um sistema sem permissão."	Website de software de antivírus (McAfee, 2019)
xxx *Hacktivists*	"Hackers que almejam fazer parte de mudanças sociais. A revelação de transgressões, ou ganhos religiosos ou políticos motivam alguns *hacktivists*."	Website de software de antivírus (McAfee, 2019)
xxx *Cyber Militias*	"[…] *cyber militia form that is organized around a central communications platform, where the members share information and tools necessary to carry out cyber attacks against their chosen adversary* […]"	Website (CCDCOE, 2020)
xxx *Zero day*	"A *zero day* exploit is a cyber-attack that occurs on the same day a weakness is discovered in the software. At that point, it's exploited before a fix becomes available from its creator."	Website de software de antivírus (kaspersky, 2020)
xxx *Denial of Service (DoS)*	*"A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning."*	(CloudFlare, 2020)
Análise Forense *Forensic Analysis*	*"Forensic analysis is the collection, analysis, and reporting of information critical to investigations by law enforcement and private organizations. Digital forensics is the application of this to digital devices, and forensic data analysis is the process of analysing digital data acquired for forensic analysis."*	(Cybrary, 2020)

Apêndice B — Quadros de apoio aos casos de estudo

Quadro 7 – Organização do ARCYBER (EUA)

Army Cyber Command		
NETCOM	*Network Enterprise Technology Command*	Opera como um provedor de serviços de informação e tecnologia de redes
1st IO *Command*	1st *Information Operations Command (land)*	Consiste numa unidade multicompetente, que disponibiliza a capacidade de desenvolver Operações de Informação e Operações no Ciberespaço
780th MI *Brigade (Cyber)*	780th *Military Intelligence Brigade (Cyber)*	Conduz Operações no ciberespaço, a fim de produzir efeitos em apoio às Operações do Exército, ou, caso tascadas para tal, em apoio a outras componentes.
CPB	*Cyber Protection Brigade*	Unidade única no Exército, tem por missão a defesa do "terreno" no ciberespaço importante, a fim de garantir a dissuasão do inimigo e garantir a liberdade de ação das forças amigas.

Fonte: Adaptado a partir de *US ARCYBER* website (2020)

Quadro 8 – Capacidades Kdo CIR (Alemanha)

CIR – capacidades mais relevantes	
Operações no Ciberespaço	Operações no Ciberespaço Ofensivas (OCO)
	Operações no Ciberespaço Defensivas (DCO)
	Apoio IT
Operações no espetro Eletromagnético	Guerra Eletrónica
	Reconhecimento Eletromagnético
Operações no Domínio das Informações	Informações Militares
	Informação Geográfica
	Operações de Comunicações
	Operações Psicológicas

Fonte: Adaptado de LTC *Chris Hoffmann Wolfram* (2019)

Apêndice C — *The Hacker Mindset* segundo *Yossi Sassi*

O Apêndice A apresenta um resumo recolhido pelo autor do presente estudo, durante a apresenta de Yossi Sassi, de Israel, no Seminário intitulado "A Ciberguerra: como travar e vencer num conflito global", organizado pelo CCD do EMGFA, no passado dia 16 de janeiro de 2020 no IUM. Yossi Sassi realizou uma apresentação subordinada ao tema "*The Hacker Mindset*" (Sassi, 2020).

Yossi Sassi, do Israel, é um dos fundadores da CyberArt, um autodenominado organismo que juntou *white hackers*, com uma vasta experiência nas tecnologias e, em simultâneos, músicos internacionais. A CyberArt realiza então trabalhos relacionados com a pesquisa na área da InfoSec e trabalhos solicitados por Instituições públicas ou privadas, para identificar possíveis lacunas nas suas redes e sistemas de informação no ciberespaço (CyberArt, 2018).

Reforçando a ideia, já apresentada no Anexo A, acerca dos diferentes tipos e motivações pelas quais se regem os hackers, é importante diferenciar o que no meio comum se conhece apenas como *hacker*, do que se designa por *white hacker*. O primeiro é mais corretamente designado por *black hacker* ou *crackers*, que é um criminoso que usa o ciberespaço, invadindo sistemas ou implantando vírus criados por si próprio ou por outrem, a fim obter vantagens, normalmente no campo financeiro. Enquanto que os *white hackers* são especialistas em segurança de sistemas e redes informacionais, que identificam lacunas nas redes ou sistemas de Instituições públicas ou privadas, a fim de produzir relatórios para que elas tenham a possibilidade de as corrigir. Geralmente estes dois grupos de *hackers* batalham entre si no ciberespaço, tendo normalmente os *black hackers* alguma vantagem.

Yossi Sassi alerta para a grande alteração de paradigma que se nos é apresentada a todos, com a possibilidade de utilização de ciber ataques, já bem identificados como uma realidade, como sendo uma arma de grande relevância no atual ambiente operacional. Esta apresenta-se com ferramentas nas suas mais diversas forças, e que, normalmente, se encontram disponíveis e acessíveis no próprio ciberespaço.

Assim, torna-se bastante importante identificar as lacunas o mais rápido possível, a fim de evitar os designados por *zero day exploit*, que são os ataques desenvolvidos assim que é identificado o ponto de entrada, mesmo antes que os próprios criadores dos sistemas o tenham feito. O que levar a que o ataque ocorra antes que seja possível o desenvolvimento, ou atualização do sistema para corrigir estas situações. A questão da atribuição, principalmente quando existe a tentativa de ligar grupos cibernéticos aos respetivos estados, é algo bastante difícil, o que permite uma margem para que alguns países apoiem determinados grupos, durante um determinado ataque, sem que o próprio estado seja envolvido.

Sassi salienta que o Reino Unido se encontra na posse de um Centro de Ciberdefesa de excelência, que se deve considerar como um país de referência na área da ciberdefesa.

Com a sociedade ligada em rede, também existe uma estreita ligação entre o SIGINT e o HUMINT, o que leva a identificar algumas questões relacionadas com os dados pessoais e a sua disponibilização na *worldwide*. Estes são disponibilizados voluntariamente por todos nós, mas temos de ter atenção aos dados que são recolhidos e processados por sistemas inteligentes, que através do nosso padrão de comportamento, cria um perfil digital. Este é utilizado por inúmeros serviços na internet, muitos deles para nosso conforto, mas a questão é que o perfil encontra-se no ciberespaço (Sassi, 2020).

Apêndice D — Espanha

Aquando da revisão da *Estrategia de Seguridad Nacional* (ESN), em 2013, a cibersegurança surge equiparada ao combate contra o terrorismo, (Gobierno de España, 2013). Tendo a questão da Cibersegurança sido identificada como um assunto de preocupação nacional, por intermédio da Lei 36/2015 de 28 de setembro, onde é incluída, na área de especial interesse de segurança nacional (Ley 36/2015, de 28 de septiembre, 2015).

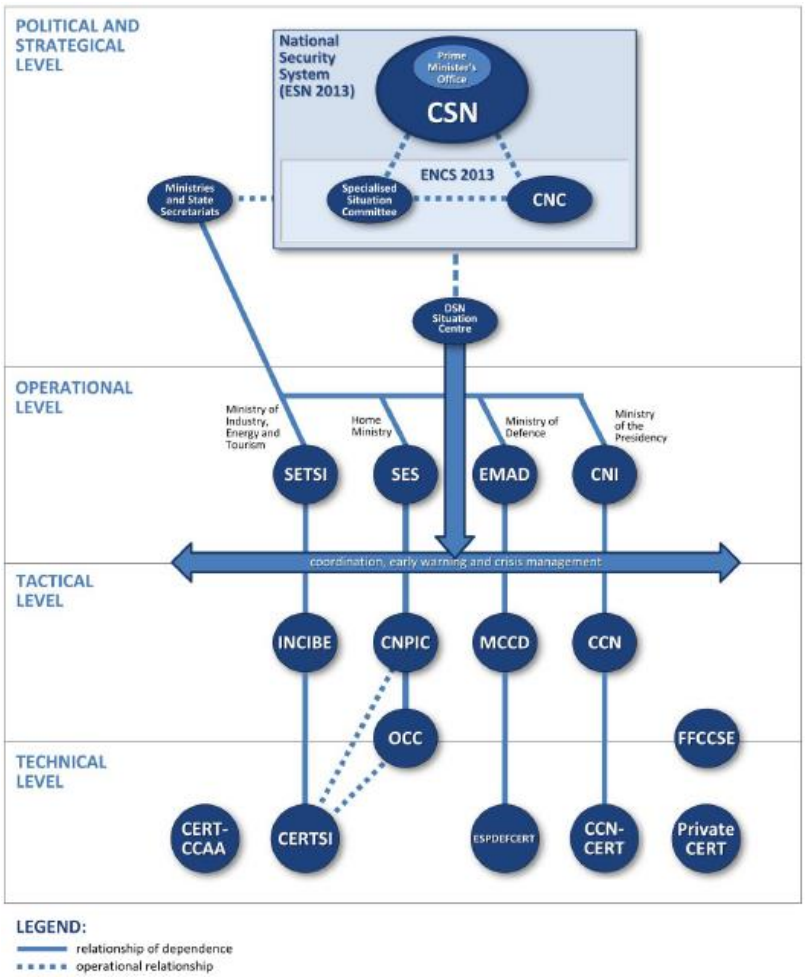


Figura 15 – Mapa Organizacional da Cibersegurança de Espanha
Fonte: Alexander Centoya (2016)

A ESN apresenta um sistema de segurança nacional em que o Primeiro Ministro assume a responsabilidade de gerir, liderar e promover a política nacional de segurança, identificando o *Consejo de Seguridad Nacional* (CSN), como o organismo central do sistema. De salientar dois organismos governamentais interligados: (i) o *Consejo Nacional de Ciberseguridad* (CNC); e (ii). o *Centro Criptológico Nacional* (CCN) (Cendoya, 2016). A capacidade de resposta do CCN para incidentes é atribuída ao CCN-CERT, que é um centro responsável por produzir os alertas de incidentes, ou potenciais incidentes, a nível nacional (Gobierno de España, 2014).

No que respeita ao nível militar, o *Mando Conjunto de Ciberdefensa* (MCCD), criado pela ordem ministerial 10/2013 de 19 de fevereiro, é o comando ciber espanhol na dependência do Ministério da Defesa. Como parte integrante do Estado-Maior conjunto de Chefes Espanhol, é o organismo responsável por comandar e coordenar as atividades na área ciber das FFAA (Cendoya, 2016).

O MCCD contribui, ao nível tático, para a resposta aos riscos e ameaças que se identifiquem para a segurança nacional, cooperando com os centros nacionais, quer com o INCIBE, quer com o CNI, na resposta a qualquer incidente relacionado com a segurança da informação. Assume a responsabilidade por definir, gerir e coordenar a *situational awareness* e as atividades de treino e formação, nesta área (Cendoya, 2016).

Figura 16 – Estrutura dos Comando de Componente das FFAA de Espanha
Fonte: Apresentação de Col Javier López de Turiso y Sánchez (2018)

O Centro para a Resposta a Incidentes de Cibersegurança (*Centro de Respuesta ante Incidentes de Ciberseguridad des Ministerio de Defensa* (ESPDEFCERT)), criado em 2014, na dependência do MCCD, é um centro operacional a nível técnico, que trabalha na defesa, exploração e resposta, com as ferramentas *forensic* laboratoriais e outras infraestruturas de pesquisa, desenvolvimento e inovação, primordialmente nas redes de comunicações e sistemas de informação pertencentes à defesa (Gobierno de España, 2014).

De acordo com o Chefe de Estado-Maior do MCCD, Col Turiso y Sánchez (2018), a cibersegurança encontra-se bastante interligada com a segurança das Informações (INFOSEC). Sendo que a ciberdefesa se entende como o conjunto de: (i) medidas focadas nas tecnologias de informação (redes de comunicações e sistemas de informação), sejam elas de prevenção, proteção ou de recuperação; (ii) e as medidas focadas nas ameaças, sejam de deteção ou de reação. Acrescenta, que as Operações Ciber, em coordenação com operações de GE e operações de influência, produzem determinados efeitos que concorrem para o alcançar dos objetivos das operações cinéticas. Num futuro próximo em que as operações se vão desenrolar num ambiente multidomínio, o controlo do ciberespaço será imprescindível para o controlo do espaço. O controlo do espaço para alcançar o controlo aéreo e quem tiver o controlo do ar, controlará a superfície (Sanchéz, 2018).

Apêndice E — Rússia

Quando a Rússia inicia o conflito com a Geórgia em 2008, existia uma grande falta de conhecimento sobre as capacidades tecnológicas das suas FFAA, nomeadamente nas áreas de CD e de GE. Em 2014, o mundo volta a ser surpreendido com a ocupação da Crimeia e com o modo demonstrado no desenvolvimento de um conflito suportado no conceito de Guerra Híbrida. Este desconhecimento, leva a que o *Internacional Centre for Defence and Security*, na Estónia, tenha desenvolvido um relatório, baseado no estudo crítico na descrição das capacidades reais, particularmente na área de GE (McDermott, 2017).

Desde que a Rússia iniciou, em 2008, a reforma de modernização das suas FFAA, que muitos estrategistas russos, elencam o conceito de guerra centrada em rede como vital para o aumento do potencial de combate militar, sendo a GE essencial para essa abordagem (Burenok, Kravchenko, & Smirnov, 2009).

> […] *There is nothing surprising that in the current circumstances, EW — as a relatively inexpensive and easily implemented means to disrupt the functioning of an enemy's radar and other systems and to defend one's own similar systems from interference — is emerging as a priority and a focus for development. In certain circumstances, use of EW approaches can be viewed as asymmetric measures that negate the benefits of an adversary's highly sophisticated systems and means of armed combat* […] (Khudoleev, 2014)

A Figura 12 apresenta a organização do conceito de GE russo, onde podemos identificar a maior especificidade por atribuídas, às diversas disciplinas da GE em comparação com os conceitos definidos pelo mundo ocidental.

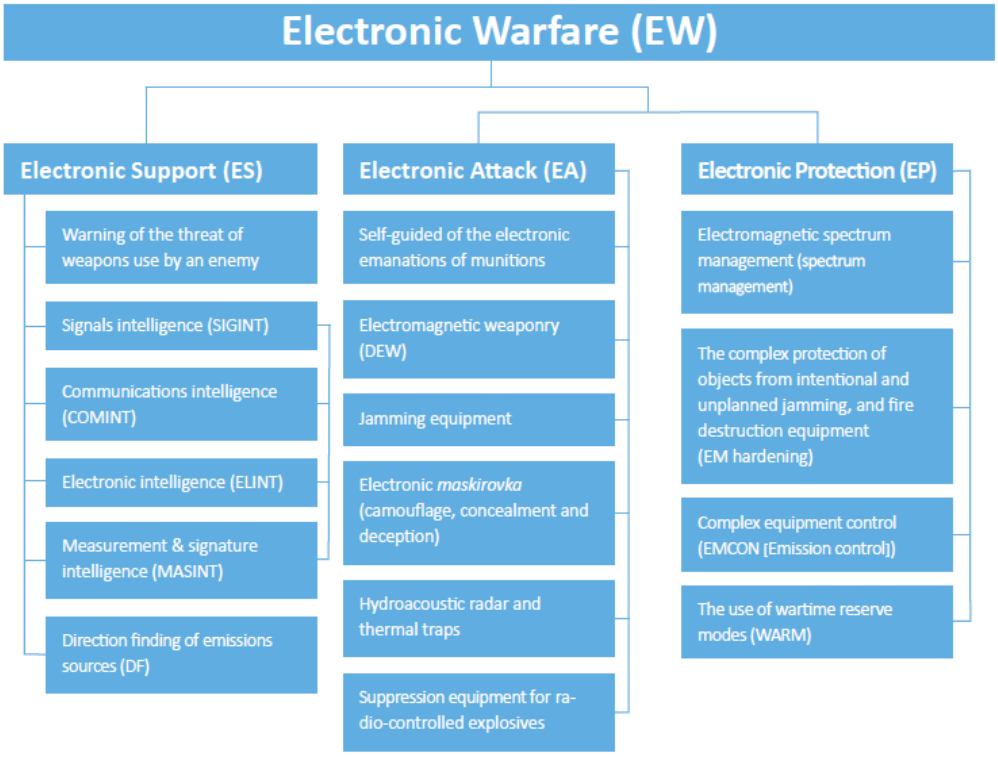


Figura 17 – Organização do conceito de GE russo
Fonte: Disponível no relatório de McDemott (2017, p. 4)

É também identificado que, dada a simbiose entre a guerra cibernética e a GE, é muito provável que ambas as capacidades sejam integradas, de forma a possibilitar a gestão e facilitar a coordenação entra ambas (McDermott, 2017).

No que respeita à estrutura de GE, em 2015 foi dado um passo importante no sentido de normalizar o apoio de GE desde o nível estratégico até ao nível tático, com a constituição da *19th EW brigade*, a sua quinta, que providência uma melhoria, nomeadamente no que respeito à melhoria nos seus equipamentos (livejournal, 2016) (McDermott, 2017).

A Rússia inclui uma unidade escalão companhia de GE na orgânica das brigadas motorizadas e de carros de combate, providenciando um alcance da sua influência de cerca de 50 km com os seus meios. Esta é uma

referência para as suas unidades da componente terrestre, devendo ser salientado que as brigadas não desenvolvem operações sem a inclusão da sua componente de GE (Silyuntsev, Demin, & Prokhorov, 2016).

A Figura 13 apresenta a orgânica tipo de uma companhia de GE.

No que respeita ao equipamento principal da companhia de GE russa, de salientar: (i) o RP-330KPK, como posto de comando VHF; (ii) o RP-330K, como estação de controlo automática; (iii) o R-378B, como estação de empastelamento de HF; (iv) o R330B, como empastelador de ligações de VHF e sistema automático de empastelamento de HF; (v) o R-330Zh, como empastelador de sistemas de comunicações satélite do tipo INMARSAT e IRIDIUM, GPS, com capacidade para empastelamento GSM e gama UHF; (vi) o RP-377U, como sistema portátil de proteção C-IED; (vii) o RP-934B, como estação de empastelamento VHF de comunicações táticas e sistemas de guiamento aéreo; (viii) o RP-377L empastelador C-IED; (ix) o RP-377LP, empastelador portátil; e (x) o RP-377UV, como empastelador automático portátil (McDermott, 2017, p. 7).

Em agosto de 2016 é realizado o exercício Elektron-2016, reconhecido como o primeiro a envolver forças de GE de todos os ramos das FFAA, desde o ano de 1979 (Defending Russia, 2016).

A fim de reforçar a ideia, acerca do valor que a Federação Russa atribuiu á componente de GE, a Figura 14 apresenta a sua distribuição geográfica, de onde podemos inferir que junto à sua fronteira com os países da EU, são colocadas 3 brigadas. Se pensarmos que, dos 29 membros da OTAN, 21 fazem parte também da EU, esta fronteira é de especial interesse para ambas as partes, tal como verificado nos anos que se seguiram, de avanços e recuos de ambas as partes, desde a queda da URSS em 1991. Se pensarmos um pouco em geopolítica, a grande ameaça de atrição entre OTAN e Rússia, situa-se exatamente nesta região, o que reforça a ideia de que a Rússia encara a necessidade da GE nas suas operações militares, pois distribui

Figura 18 – Distribuição geográficas das Brigadas de GE russas
Fonte: Disponível no relatório de McDemott (2017, p. 8)

Atualmente o grande paradigma entre os especialistas militares russos, encontra-se focado na futura, possível sinergia entre a GE e a capacidade de guerra centrada em rede, associando deste modo a GE com as operações desenvolvidas no ciberespaço. Esta mudança de paradigma reforça a importância de possuir uma abordagem de adoção de acompanhamento na evolução das capacidades de GE, identificada como um enabler importantíssimo no potencial de combate de uma força, e que poderá num futuro próximo desequilibrar a balança OTAN-Rússia (McDermott, 2017).