INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO PROMOÇÃO A OFICIAL SUPERIOR
2020/2021, 2.ª EDIÇÃO

TII

A CAPACIDADE DE SIGNAL INTELLIGENCE E DE GUERRA ELETRÓNICA NAS FORÇAS ARMADAS

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

António Alexandre Ramos Maia
Primeiro-tenente, STAEL

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A CAPACIDADE DE SIGNAL INTELLIGENCE E DE GUERRA ELETRÓNICA NAS FORÇAS ARMADAS

PRIMEIRO-TENENTE, STAEL António Alexandre Ramos Maia

Trabalho de Investigação Individual do CPOS-M 2020/2021

2ª Edição

Pedrouços 2021

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

A CAPACIDADE DE SIGNAL INTELLIGENCE E DE GUERRA ELETRÓNICA NAS FORÇAS ARMADAS

PRIMEIRO-TENENTE, STAEL António Alexandre Ramos Maia

Trabalho de Investigação Individual do CPOS-M 2020/2021

2ª Edição

Orientador: MAJ/ENGEL Luís Filipe de Jesus Fernandes

Pedrouços 2021

Declaração de compromisso Antiplágio

Eu, **António Alexandre Ramos Maia**, declaro por minha honra que o documento intitulado **A capacidade de *Signal Intelligence* e de Guerra Eletrónica nas FFAA** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **CPOS M 2020/2021 – 2ª Edição** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

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

Pedrouços**, 22** de **julho** de **2021**

António Alexandre Ramos Maia

Agradecimentos

Agradeço ao meu orientador, MAJ Jesus Fernandes, pela total disponibilidade, ajuda e apoio com os seus preciosos conselhos e orientações, que me guiaram e contribuíram significativamente para o sucesso na elaboração deste trabalho..

Uma palavra especial de gratidão a todos os camaradas que tiveram a amabilidade de, despendendo do seu tempo, para me ajudar, respondendo ao questionário, fornecendo dados e também encorajar na prossecução deste trabalho – MAJ Rodrigues de Freitas, CAP Humberto Costa e 1TEN Pessoa Baptista o meu muito obrigado.

A todos os oficiais que de uma forma direta ou indireta me ajudaram durante este curso e na realização deste trabalho, indicando qual o caminho a seguir e a quem me socorrer para a conclusão desta investigação: VALM Silvestre Correia, CMG Cavaleiro Ângelo, CMG Pais Neto, CFR Cavaleiro Ângelo, CFR Vieira Serra, MAJ Silva Boita.

Aos meus filhos, Rúben e Matilde, obrigado por estarem sempre felizes, mesmo quando a minha falta de tempo me impediu de vos dar a atenção que merecem.

E finalmente, a ti, Márcia, por todo o amor, carinho, paciência e incentivo ao longo deste desafio e por acreditares sempre em mim. Sem ti, nem curso com sucesso, nem trabalho acabado! Obrigado!

Índice

Índice de Figuras

Índice de Quadros

Resumo

Num mundo onde a evolução tecnológica avança rapidamente e em que as telecomunicações e redes móveis deram um salto tecnológico significativo neste início do século, não podemos descurar dois conceitos muito importantes no seio militar e que põem a descoberto as vulnerabilidades de uma nação colocando em risco muitos militares e civis de ambos lados de uma guerra. Esses conceitos são SIGINT e EW que nas últimas duas décadas alteraram o paradigma da segurança e defesa internacional, obrigando à adoção de novas estratégias, metodologias de ação e capacidades tecnológicas mais avançadas. A transversalidade destas componentes aplicadas aos diversos meios e sistemas torna-os numa arma letal e silenciosa extrapolando o que se poderia imaginar há vinte anos atrás. Desta forma surgiu a necessidade de criação de um novo conceito em que envolve as diferentes áreas de ação e interoperabilidade dos diversos atores quer em forças combinadas ou conjuntas.

Para alcançar o objetivo do presente trabalho será apresentada uma base concetual de referência, que além de explanar os conceitos, identifica a estrutura existente na *North Atlantic Treaty Organization* (NATO), seguindo a mesma organização estrutural, mas para dois países com o intuito de estabelecer diferentes casos de estudo, terminando com a realidade nacional. Em termos conclusivos surge a proposta de edificação de uma capacidade para efetuar operações conjuntas e partilha de conhecimentos e meios.

Palavras-chave: SIGINT, EW, NATO

Abstract

In a world where the technology evolution is changing fast and in which telecommunications and mobile networks have taken an significant technological leap in the beginning of the century, we cannot overlook two very important concepts in the military branch, which expose the vulnerabilities of a nation, and puts many military and civilian on both sides of a war at risk. These concepts are SIGINT and EW that in the last two decades have changed the paradigm of international security and defense, forcing the adoption of new strategies, methodologies and more advanced technological capabilities. The transversality of these components applied to the various media and systems make them a lethal and silent weapon, extrapolating what could have been imagined twenty years ago. In this way, a new concept arises involving the different areas of action and interoperability of the different actors, whether in combined or joint forces.

To achieve the objective of the present work, the base conceptual reference will be presented, in addition to explaining the concepts, identifying the existing structure in the North Atlantic Treaty Organization (NATO), following the same structural organization, specifically for two different countries to establish different cases of study, ending with the national reality. As a conclusion, this work offers a proposal to build a capability to carry out joint operations and share knowledge and resources.

Keywords: *SIGINT, EW, NATO*

Lista de abreviaturas, siglas e acrónimos

B

BD	Base de Dados
BDN	Base de Dados Nacional

C

C4ISR	*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*
CADOP	Centro de Gestão e Análise de Dados Operacionais
CECM	*Communications ECM*
CEMA	*Cyber-Electromagnetic Activities*
CESM	*Communications ESM*
CGE	Centro de Guerra Eletrónica
CMS	*Combat Management System*
COMINT	*Communication Intelligence*
CompGE	Companhia de Guerra Eletrónica
CTGE	Centro de Treino de Guerra Eletrónica
C-UAS	*Communications Unmanned Aerial Systems*

D

DISA	*Defense Information Systems Agency*
DoD	*Department of Defense*
DSO	*Defense Spectrum Organization*

E

E3	*Electromagnetic Enviromental Effects*
EA	*Electronic Attack*
ECM	*Electronic Counter Measures*
ED	*Electromagnetic Defence*
EDGE	Equipas Destacáveis de Guerra Eletrónica
EEM	Espectro Eletromagnético
ELINT	*Electronic Intelligence*

EME	*Electromagnetic Environment*
EMGFA	Estado-Maior-General das Forças Armadas
EOB	*Electronic Order of Battle*
ES	*Electronic Surveillance*
ESM	*Electronic Warfare Support Measures*
EW	*Electronic Warfare*
EXE	Exército

F

FAP	Força Aérea Portuguesa
FFAA	Forças Armadas

I

IMINT	*Imagery Intelligence*
INTEL	*Intelligence*
IUM	Instituto Universitário Militar

J

JEWCS	*Joint Electronic Warfare Core Staff*

M

MAR	Marinha Portuguesa
MC	*Military Committee*
MIC	Metodologia de Investigação Científica
MILREP	*Military Representative*
MLU	*Mid-Life Upgrade*

N

NATO	*North Atlantic Treaty Organization*
NEDB	*NATO Emitter DataBase*
NEDBAG	*NATO Emitter DataBase Advisory Group*
NEDB-NG	*NATO Emitter DataBase-Next Generation*
NEWAC	*NATO Electronic Warfare Advisory Committee*

NSA	*National Security Agency*
O	
OE	Objetivo Específico
OG	Objetivo Geral
Q	
QC	Questão Central
QD	Questão Derivada
R	
RFI	*Request For Information*
S	
SEWOC	*SIGINT & EW Operations Centre*
SIGIDOP	Sistema de Gestão Integrado de Dados Operacionais
SIGINT	*Signal Intelligence*
T	
TII	Trabalho de Investigação Individual
TO	Teatro de Operações
TTP	*Technical, Tactical and Procedures*

1. Introdução

> *"A guerra eletrónica é uma "guerra" em rápida evolução e que está constantemente a ganhar relevância relativamente às outras "guerras", à medida que as nações buscam obter vantagem na próxima geração de tecnologia de conflito."* (O'CONNELL),

As capacidades de Guerra Eletrónica (EW)[1] estão a tornar-se numa necessidade inestimável em situações de combate. O aviso antecipado, busca, interceção, localização, deteção e aquisição de alvos são tarefas primordiais para a EW.

Os cenários de combate mudam rapidamente devido a novas ameaças que estão a ser desenvolvidas diariamente, enquanto as defesas são testadas com base no espectro eletromagnético (EEM). Na EW, é necessário detetar, validar e processar os dados vindo de origens diferentes e identificá-los rapidamente para saber se são de fontes amigas, hostis ou, o mais indesejado, de fontes desconhecidas, para que as decisões sejam as mais assertivas. O sucesso da missão agora requer um conhecimento ainda mais abrangente do EEM (Cullen, 2014).

Se por um lado a *North Atlantic Treaty Organization* (NATO) tem uma boa visão sobre as ameaças que pode encontrar em terra, no mar, no meio subaquático, no ar e no espaço, por outro lado o ciberespaço é cada vez mais uma área que não é totalmente conhecida e por esta razão muitas nações continuam a desenvolver novos sistemas de armas para operar nessas dimensões, mas infelizmente, as iniciativas da NATO, em muitos casos, não se desenvolveram nem adaptaram a disciplina da EW para uma nova realidade. Uma geração de militares e de profissionais cresceu negligenciando as vulnerabilidades inerentes à dependência operacional do EEM e hoje a "guerra" faz-se utilizando essa componente (Spreckelsen, 2018).

Pelas razões atrás descritas e tendo como base a evolução dos sistemas de EW e consequentemente da componente de *Signal Intelligence* (SIGINT) quer das nações que pertencem à NATO quer das nações não-NATO e por outro lado, com o intuito de saber qual o estado da arte em relação à organização e as capacidades existentes nas nossas Forças Armadas (FFAA), uma vez que estando Portugal integrado na organização NATO

[1] Neste trabalho iremos utilizar a terminologia de Guerra Eletrónica utilizada e conhecida no meio das Operações. Neste sentido utilizar-se-á a terminologia em Inglês nos termos técnico de Guerra Eletrónica.

obrigando-o por isso a cumprir com os requisitos definidos por esta organização, pretende-se com esta investigação identificar as capacidades presentes e futuras de SIGINT e de EW em cada ramo, assim como a sua organização interna, por forma acomodar sinergias entre os mesmos dotando-os para uma realidade que presentemente não existe no conceito nacional, tendo em vista uma cooperação conjunta entre ramos nos exercícios nacionais ou em Teatro de Operações (TO) que venham a ser empenhados sobre a supervisão de uma entidade como é o caso do Estado-Maior-General das Forças Armadas (EMGFA), indo também ao encontro do que está a ser revisto e recentemente divulgado na Proposta de alteração da Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA) (Presidência do Conselho de Ministros, 2021).

Para alcançar o objetivo desta investigação apresentou-se como base concetual de referência, os conceitos, identificando a estrutura e capacidade da NATO nesta área, ao que se seguiu, utilizando a mesma organização estrutural no que se referente a diversos países, com o intuito de estabelecer diferentes casos de estudo. Por fim apresentou-se a realidade nacional de SIGINT e de EW assim como a estrutura organizacional existente em cada ramo.

Para termo de comparação foram utilizadas as estruturas atrás identificadas, mostrando diferentes realidades de forma que nos possamos organizar, com o objetivo de edificar uma força militar conjunta para poder operar num ambiente com estas valências.

Podemos desde já referir que a nível nacional, por exemplo, na Marinha (MAR) com o aumento ao efetivo dos submarinos da classe Tridente em 2010, a capacidade SIGINT aumentou de uma forma exponencial e na superfície, atualmente com a *Mid-Life Upgrade* (MLU) das fragatas da classe Bartolomeu Dias surgem novos equipamento de EW e eletro-óticos (EO) aliados a um novo sistema de combate (CMS) *Guardion*, permitindo uma superioridade na recolha de informação que até agora era inexistente nas unidades de superfície, fazendo com que a MAR possa ombrear com as outras nações aliadas, na exploração, analise, desenvolvimento e *Tecnical Tactical Procedures* (TTP) nesta área. No Exército (EXE) a aquisição dos equipamentos de COMINT - DDF 1555, a capacidade de SIGINT fica a par com o que é reconhecido pela NATO como equipamentos de última geração. No que respeita à Força Aérea Portuguesa (FAP) a aquisição da nova aeronave KC-390 aliado ao novo equipamento de EW SPS-45(V)5 resulta numa modernização há muito esperada e que só o treino não basta para poder retirar o máximo das capacidades destes meios, sendo para isso necessário a realização de exercícios conjuntos, para os ramos

poderem validar as suas TTP e só assim é que poderão demonstrar estarem à altura, ao nível operacional e tático, relativamente a outras nações, na área de SIGINT e EW.

Face ao exposto, verifica-se a necessidade de evidenciar as capacidades de SIGINT e de EW nos ramos das FFAA de modo a maximizar a interoperabilidade entre estes, com a finalidade de prepará-los para um cenário real com as forças aliadas, explorando de forma eficiente os recursos entre as entidades, para racionalização de meios e recursos e consequentemente a redução de custos.

Neste estudo iremos caracterizar a estrutura SIGINT e EW, existente em dois países, que servirão de exemplo pelas boas práticas utilizadas e que poderão ajudar na caracterização de uma solução a aplicar no caso português. São eles os Estados Unidos da América e a Alemanha. Quanto ao primeiro a escolha recaiu por ser uma superpotência a nível mundial em que a sua organização assim como as suas capacidades e experiência servem de exemplo a muitas outras nações. O outro país escolhido para este estudo é a Alemanha, por ser uma das nações na linha da frente quanto ao investimento que está a ser feito na modernização das suas tropas ao que esta capacidade diz respeito, pelo que criou uma organização diferente da norte-americana, mas igualmente eficaz no seio operacional.

Face às entrevistas exploratórias realizadas, identificou-se um problema concreto, que passa por uma inexistência na gestão de operações conjuntas na congregação das sinergias para obtenção do sucesso da missão.

Assim sendo, o Objetivo Geral (OG) desta investigação consiste em analisar possíveis caminhos de implementação de arquitetura de interoperabilidade de SIGINT e de EW ao nível militar conjunto. Para tal, será necessário conhecer as capacidades de cada um dos ramos, tanto as presentes como as futuras, bem como identificar as possíveis melhorias na racionalização dos meios, a fim de permitir uma melhor participação conjunta na condução de operações militares.

De modo a alcançar o (OG) da investigação, foram elencados os seguintes objetivos específicos (OE):

OE1: Caracterizar as estruturas de SIGINT e de EW na NATO.

OE2: Caracterizar as estruturas de SIGINT e de EW dos Estados Unidos da América e da Alemanha.

OE3: Caraterizar as estruturas de SIGINT e de EW dos três ramos das FFAA.

Com base no problema já definido e nos objetivos atrás enunciados, o objeto da investigação e os objetivos (geral e específicos) é formulada a seguinte questão central (QC) para atingir o OG proposto:

Que principais características deve ter o modelo de implementação de uma arquitetura de interoperabilidade de SIGINT e de EW no nível militar conjunto?

Para alcançar os objetivos delineados, o estudo encontra-se estruturado da seguinte forma: o enquadramento, justificação do tema, objeto de estudo e sua delimitação farão parte da introdução. Por outro lado, também iremos descrever os objetivos e as questões da investigação, assim como uma breve síntese da metodologia de investigação. Os três capítulos seguintes cumprem com os requisitos dos OE de forma a responderem às QD, e, por último, as conclusões onde para além de expor as ideias também contempla uma sugestão de organização e concentração de sinergias para as nossas FFAA.

1.1. Enquadramento teórico e concetual

De seguida iremos abordar os aspetos essenciais de investigação, entre eles o contexto e os conceitos estruturantes, decorrentes do estudo para o trabalho desenvolvido nesta "arte da guerra" que é a SIGINT e a EW, inserindas nas Ciências Militares.

1.1.1. Contexto

Se por um lado a EW utiliza toda a extensão do EEM para conduzir operações de empastelamento, para negação desse mesmo espetro a um dado oponente ou obter aviso antecipado através da interceção de determinadas emissões paramétricas de interesse – ELINT (*Electronic Intelligence*), por outro lado a COMINT (*Comunication Intelligence*), cujas interceções de comunicações do vasto espetro radioelétrico são analisadas, correlacionadas e transformadas em conhecimento. O racional é um agente emissor que será catalogado segundo as características especificas da sua emissão, localização geográfica (azimute e/ou posição), intervalo temporal, procedimentos, política de transmissões, etc., para depois ser etiquetado numa Base de Dados (BD) como emissor de interesse, pelo que o torna noutra das disciplinas das Informações. Ao congregar as duas (ELINT e COMINT) obtemos a SIGINT (Nieto, 2016).

As sensibilidades associadas ao COMINT geralmente requerem classificações de segurança mais altas (COSMIC TOP SECRET) para salvaguarda da informação nela contida, por outro lado a ELINT, por si só e apesar de ser considerada como uma subdisciplina da SIGINT, quase sempre a sua classificação de segurança é SECRETO. No entanto, o estabelecimento de uma capacidade combinada de EW e SIGINT totalmente

integrada e adaptada à missão é um passo valioso para agregar melhor essas duas componentes intimamente relacionadas, proporcionando um uso mais eficiente e eficaz de recursos escassos. A coordenação e o uso competente desses recursos por um lado e a partilha de dados e sensores por outro vão definir o SEWOC (*SIGINT and Electronic Warfare Operation Center*) como um 'multiplicador de força', sendo, portanto, considerada a configuração ideal para as operações (MC 0515, 2012).

Assim sendo, este trabalho de investigação visa contribuir para o esclarecimento das capacidades supracitadas nos três ramos das FFAA, identificando-as quer as atuais quer as futuras, assim como a forma que estão organizados e a possibilidade de interoperabilidade entre os mesmos podendo vir a ser criada uma estrutura robusta destas capacidades no EMGFA para apoio às operações conjuntas e a criação de uma BD única a nível nacional.

1.1.2. Conceitos estruturantes

Por forma a alcançar o objetivo central da nossa investigação e identificar a "Capacidade de SIGINT e de EW nas FFAA" torna-se necessário definir antecipadamente alguns conceitos estruturantes, essenciais para a compreensão do desenvolvimento da nossa tese, salientando-se os seguintes:

A EW é definida como sendo a ação militar que explora o espectro eletromagnético, englobando a interceção e a identificação de emissões eletromagnéticas, o emprego de energia eletromagnética com a finalidade de reduzir ou impedir o uso hostil do espectro eletromagnético e as ações que garantam o seu uso efetivo pelas nossas forças. (PEMGFA/GE1, 1994, Anexo A).

Atendendo à evolução da nova política e doutrina da NATO para operações no *Eletromagnetic Environment* (EME) e tendo como base a mudança de conceito elaborado no "*Military committee transformation concept for future NATO Eletronic Warfare*" (MCM-0142, 2007), são apresentadas as seguintes terminologias:

Electronic Attack (EA): uso de energia eletromagnética, de armas antirradiação para atacar pessoas, instalações ou equipamentos com a intenção de degradar, neutralizar ou destruir a capacidade de combate do inimigo. Ao conjunto de medidas tomadas para impedir ou reduzir a eficiente utilização do EEM por parte do inimigo, através da utilização de energia eletromagnética chamamos *Electronic Counter Measures* (ECM) (MCM-0142, 2007). As medidas mais utilizadas são:

- ***Jamming***: empastelamento eletrónico, que consiste na deliberada radiação, re-irradiação ou reflexão de energia eletromagnética, com o objetivo de reduzir a

eficácia da utilização pelo inimigo de dispositivos, equipamentos ou sistemas eletrónicos, podendo ser utilizadas contra estações de Comando e Controlo, radares ou provocar interferência nas comunicações (MCM-0142, 2007);

- ***Electronic Deception***: tem como objetivo confundir, distrair ou seduzir o inimigo ou os seus sistemas eletrónicos com envio de informação falsa (i.e., ecos falsos) através do EEM (MCM-0142, 2007).

Electronic Defence (ED): utilização do EEM para proteção da força amiga, ou seja, são ações que visam a proteção do pessoal, instalações e equipamentos de quaisquer efeitos do uso do EEM pelo inimigo com intenção de degradar, neutralizar ou destruir a capacidade de combate aliado uma vez que tanto a força amiga como inimiga utilizam o mesmo espectro eletromagnético. Neste caso as medidas de proteção utilizadas, as *Electronic Protective Measures* (EPM) que fazem parte da componente de EW (MCM-0142, 2007), estão divididas em duas partes:

- **EPM ativas**: medidas detetáveis, como por exemplo a alteração dos parâmetros dos equipamentos ativos, de modo a assegurar uma utilização efetiva do EEM pelas forças amiga ou a utilização de engodos e/ou flares (nuvens de Chaff), simulando a silhueta de um navio ou de uma aeronave para enganar o míssil ou a utilização de frequências especificas e pré-determinadas de certos equipamentos de defesa (MCM-0142, 2007);
- **EPM passivas**: medidas não detetáveis, como por exemplo os procedimentos ou características técnicas dos equipamentos, de modo a garantir a efetiva utilização do espectro eletromagnético pelas forças amigas. Neste caso através do controlo da política de emissões para que cada unidade da força saiba que frequências pode utilizar e em que período (MCM-0142, 2007).

Electronic Surveillance (ES): utiliza o EEM para pesquisar, intercetar, identificar e localizar fontes de energia eletromagnética irradiada intencionalmente para fins de reconhecimento imediato das ameaças, seleção de alvos, planeamento e condução de operações futuras. A medida utilizada neste campo é a *Electronic Support Measures* (ESM) (MCM-0142, 2007). A ESM compara os sinais detetados pelos equipamentos de SIGINT e/ou EW com as informações que estão programadas nos sistemas de combate, chamadas EOB (*Electronic Order of Battle*) com o intuito de reconhecer quem está a irradiar no espectro envolvente (Cullen 2014).

Os dados recolhidos no EEM são compilados pelos equipamentos de guerra eletrónica para serem posteriormente analisados nos respetivos centros e validados por forma a serem alimentadas as Bases de Dados (BD) nacionais. A nível nacional, cada ramo é detentor de uma BD, onde valida e guarda a informação recolhida comparando-a com a que existe na base de dados da NATO que é o *Nato Emitter Data Base* (NEDB).

Em Portugal não existe uma entidade que centralize os dados por forma a ter uma BD nacional em que todos os dados recolhidos, analisados e validados, fossem submetidos por forma a serem guardados e geridos, salvo melhor opinião, pelo EMGFA, sendo que alguma da informação que é validada por cada ramo é posteriormente submetida para o NEDB. Esta BD da NATO é alimentada e partilhada por 21 nações, estando neste momento em fase de conclusão uma nova BD, que é o *Nato Emitter Data Base-Next Generation* (NEDB-NG), onde contemplará não só os dados de ELINT, com informação paramétrica dos radares e dos EO (eletro-óticos), mas também informação de COMINT. Toda a informação contida na BD serve para alimentar os sistemas de combate dos diversos sistemas aquando da criação das EOB. Por esta razão os dados nela contida têm de ser os mais fiáveis e atualizados possíveis (Spreckelsen, 2019).

Em suma, o espaço eletromagnético onde tudo se desenrola é o *Electromagnetic Enviroment* (EME). Neste "espaço invisível" vamos encontrar as frequências dos radares, das telecomunicações quer sejam elas em claro ou em cifrado, as comunicações das redes móveis, GPS (*global positioning system*), etc. (Nieto, 2016).

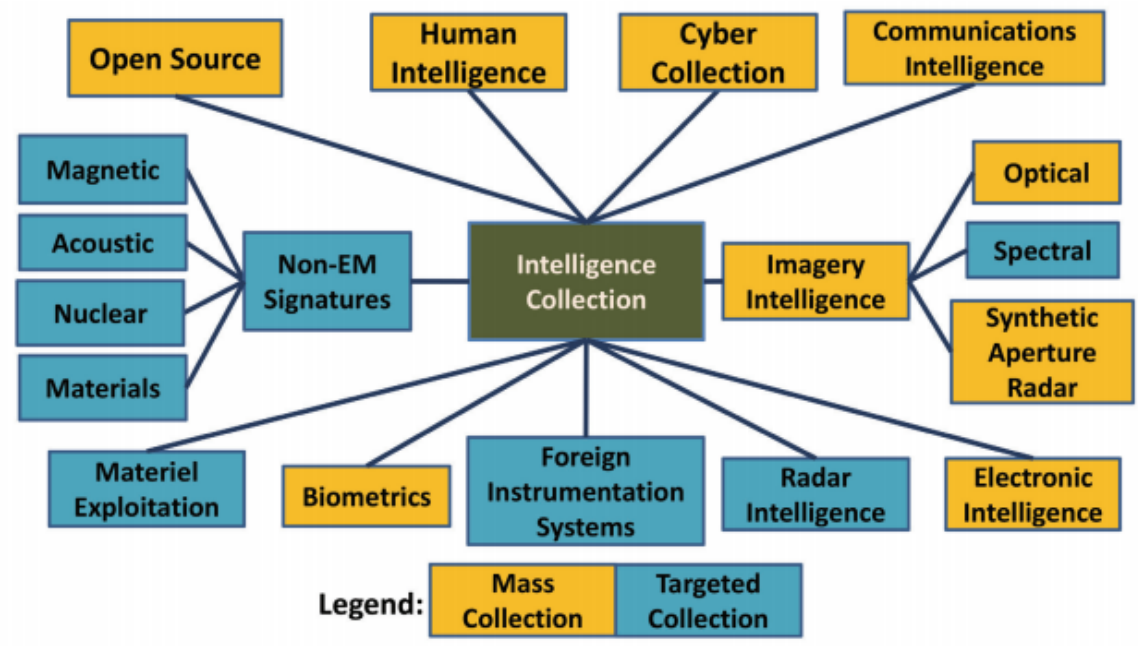

Figura 1 - Disciplinas de recolha de Informação

Fonte: Clark (2013)

1.2. Modelo de análise

A presente investigação regeu-se pelo modelo de análise demonstrado no Quadro 1.

Quadro 1 – Modelo de análise

Objeto	A organização e as capacidades de SIGINT e de EW dos três ramos das FFAA enquadradas com as capacidades da NATO e dos países que servirão para os casos de estudo		
Delimitação	Temporal: Desde 2010 à atualidade		
	Espacial: Espectro Eletromagnético		
	Conteúdo: SIGINT, GE, Cyber, INTEL		
Estratégia	Qualitativa		
Raciocínio	Dedutivo		
Design de pesquisa	Grounded Theory		
Objetivo Geral	**Questão Central**	**Conceitos**	**Técnicas de análise e discussão de dados**
ANALISAR possíveis caminhos de implementação de arquitetura de interoperabilidade de SIGINT e de EW ao nível militar conjunto	Que principais características deve ter modelo de implementação de uma arquitetura de interoperabilidade de SIGINT e de EW no nível militar conjunto?	Capacidade SIGINT Capacidade EW Interoperabilidade	- Análise documental
Objetivos Específicos	**Questões Derivadas**	**Conceitos**	**Técnicas de recolha e tratamento de dados**
Caracterizar as estruturas de SIGINT e de EW na NATO	Como se caracterizam as estruturas de SIGINT e de EW na NATO?	Capacidade SIGINT Capacidade EW Interoperabilidade	- Pesquisa documental
Caracterizar as estruturas de SIGINT e de EW dos Estados Unidos da América e da Alemanha	Como se caracterizam as estruturas de SIGINT e de EW dos Estados Unidos da América e da Alemanha?		- Pesquisa documental - Entrevista semi-estruturada
Caracterizar as estruturas de SIGINT e de EW dos três ramos das FFAA	Como se caracterizam as estruturas de SIGINT e de EW nos três ramos das FFAA?		

1.3. Metodologia e método

Iremos agora apresentar a metodologia e o método seguido por esta investigação, assim como os seus participantes e procedimentos, instrumentos de recolha de dados e por fim as técnicas utilizadas no tratamento de dados.

1.3.1. Metodologia

Este método segue as Orientações Metodológicas lecionadas nas aulas de MIC e utilizado no Instituto Universitário Militar (IUM, 2021).

Para este trabalho de investigação irá ser utilizado o método de raciocínio Dedutivo, visto que se trata de um tema concreto, de natureza técnica e aplicada, em que serão recolhidas, comparadas e caracterizadas as melhores práticas de SIGINT e EW a nível internacional, com a finalidade de as adaptar ao caso concreto da estrutura militar conjunta nacional.

Relativamente à estratégia desta investigação, optou-se por uma estratégia qualitativa, em que as técnicas de recolha de dados e instrumentação serão as entrevistas e a observação baseada na análise documental, visando a resposta à QC.

Para analisar e consolidar toda a informação recolhida, foram também realizadas entrevistas exploratórias aos especialistas nesta área dos três ramos das FFAA, pretendendo-se explanar as diferentes estruturas a nível nacional por um lado e por outro recorrendo ao

nível documental de fontes abertas, sites NATO classificados e a troca de emails com militares e civis estrangeiros de nações congéneres, para que possamos ter um quadro macro e propor um modelo que melhor se adeque à realidade portuguesa por forma a responder às QD e à QC.

Na seguinte figura apresentamos o desenho de pesquisa utilizado neste estudo, que assenta no *Grounded Therory* em foi efetuado o levantamento de diferentes tipos de organização existente na área de SIGINT e EW e baseado nesse pressuposto foi criado um modelo que poderá ser testado nas nossas FFAA verificando a sua exequibilidade. Se tal não for possível terá de ser corrigido esse modelo até obter um resultado satisfatório. Aquando da sua saturação quer por não obedecer ao requisito de adequabilidade ou por existirem novas tipologias de organização, teremos de voltar ao terreno para verificar o que se está a fazer e começamos todo o processo de novo.

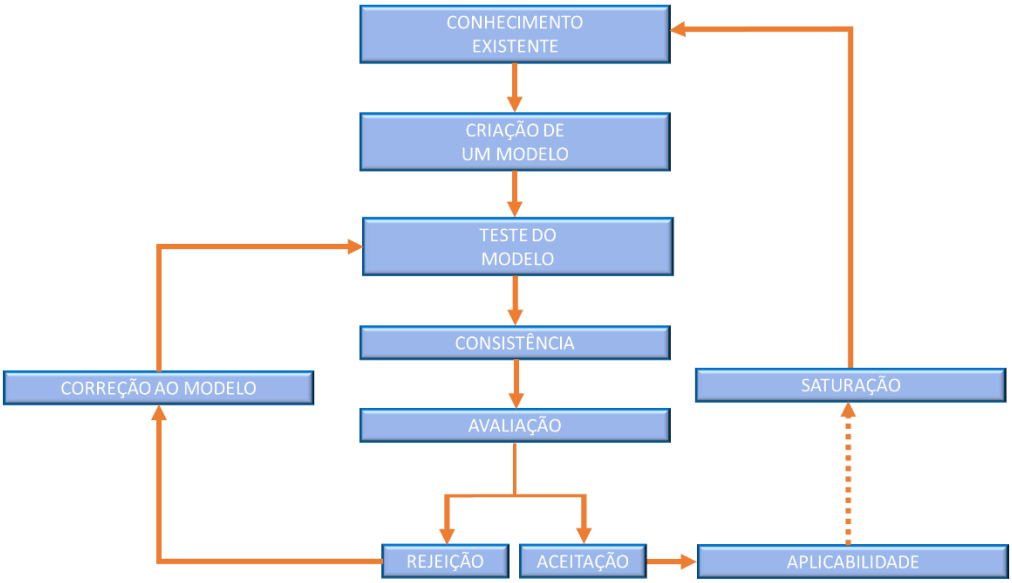

Figura 2 – Desenho de pesquisa

1.3.2. Participantes e procedimento

Este estudo integrou os principais intervenientes com responsabilidade e experiência direta nas áreas de SIGINT e EW nos três ramos das FFAA, conforme identificados no Quadro 2. As suas intervenções ocorreram na fase de recolha de dados através de entrevistas semiestruturadas, sendo os seus conteúdos desenvolvidos ao longo do capítulo 4.

Quadro 2 – Matriz de Entrevistados

Posto/Esp.	Nome	Organismo/Serviço	Data
MAJ ENGEL	Nuno Freitas	Centro de Guerra Eletrónica FAP	31JAN21
CAP Tm	Humberto Costa	Companhia de Guerra Eletrónica EXE	08JAN21
1TEN STAEL	Pessoa Baptista	Centro de Gestão e Análise Operacional MAR	12JAN21

Quanto ao procedimento adotado, foi estabelecido contato telefónico para a condução da entrevista e correio eletrónico para a validação da sua transcrição.

1.3.3. Objeto de estudo e sua delimitação

O objeto da investigação deste trabalho é a organização e as capacidades de SIGINT e de EW dos três ramos das FFAA enquadradas com as capacidades da NATO e dos países, atrás referidos que vão servir para os casos de estudo.

Relativamente à delimitação temporal, poder-se-á identificar alguns momentos-chave que permitam enquadrar a investigação. O primeiro prende-se com o aumento ao efetivo naval dos submarinos da classe Tridente em 2010, noutro plano colocaremos a MLU das fragatas Bartolomeu Dias iniciado em 2018 prevendo-se a chegada da primeira fragata já modernizada no primeiro semestre de 2021. No Exército podemos referenciar o ano de 2020 como o ressurgimento da capacidade EW, devido ao fato de voltarem a ter valências na área da formação desta capacidade com o "Curso de Fundamentos de GE", que após alguns anos de interregno voltou a ser lecionado abrindo agora as portas aos outros dois ramos das FFAA com o intuito de aproximar e desenvolver sinergias entre os ramos nesta capacidade. Na FAP, o ano de 2021, marca um ponto de viragem com a aquisição de novos meios quer a nível de equipamento de EW quer ao nível aeronáutico com a aquisição das novas aeronaves KC-390 para substituição dos C-130H.

No plano externo, em concreto, a criação de uma nova BD de SIGINT, o NEDB-NG, no corrente ano de 2021, quer a nível da formação quer a nível operacional, esta ferramenta será distribuída às nações NATO, criando assim mais um *asset* ao serviço desta organização e consequentemente das nações que dela dependem, reforçando a capacidade de conhecer quem está a nossa volta no EME aquando das diversas missões tanto a nível nacional, como em forças conjuntas num TO (Steven, 2014).

Quanto à delimitação espacial, a partir deste tema pode-se imediatamente delimitar todo EEM que serve de sustentação quer à EW assim como ao nível do SIGINT.

2. Estrutura SIGINT e EW da NATO

Neste capítulo iremos abordar a estrutura e a capacidade SIGINT e EW na NATO, identificando possíveis casos de aplicabilidade no nosso país.

Na NATO o organismo responsável pela doutrina, conceitos e desenvolvimento da política de Comando e Controlo (C2) é o *NATO Eletronic Warfare Advisory Committee* (NEWAC), assim como também pela monitorização e apoio às operações desenvolvidas pela aliança no âmbito da EW. A composição deste comité é feita por todos os países pertencentes à NATO ao nível do Comando Estratégico (NATO, 2011). Ao realizar ações que visem a exploração do espetro eletromagnético que forneçam *situational awareness* e alerta das ameaças por forma a preparação dos efeitos ofensivos e defensivos, torna este como o seu objetivo principal. (Nieto, 2016)

Se falarmos a nível de SIGINT o organismo responsável pela doutrina, conceitos, requisitos de treino e políticas é o *NATO Advisory Committee on SIGINT* (NACSI), sendo a sua composição também feita pelas nações pertencentes à NATO. O objetivo principal é a recolha de informação INTEL a nível de COMINT, incluindo a *situational awareness* e a avaliação de ameaça, para que que a tomada de decisão seja a mais assertiva, para elaboração dos produtos de INTEL, tomadas de decisão e na resposta aos *Request For Information* (RFI) (Nieto, 2016).

Estas duas entidades estão sob a alçada do *Military Committee* (MC), que é a autoridade máxima ao nível estratégico da NATO, composto por 30 militares (MILREP)[2] das nações NATO, exceto a Islândia que o seu representante é civil (NATO, 2021, 10 de junho).

A política EW é coberta pelo MC 0064 da NATO. Esta doutrina tem sido revista regularmente para acompanhar as mudanças no ambiente eletromagnético e operacional, quer na Estrutura de Comando da NATO quer nas ameaças que a Aliança enfrenta. Esta política é acordada por todos os Aliados e fornece a orientação abrangente necessária para formular uma doutrina comum e padrões de interoperabilidade (NATO, 2021, 06 de abril).

Existem ainda mais três atores importantes para este estudo, que passaremos a descrever de seguida:

- **NEDBAG** – *NATO Emitter DataBase Advisory Group*, entidade responsável por efetuar o desenvolvimento e a manutenção da base de dados da NATO que é o NEDB, assim como o aconselhamento técnico tendo em vista a compatibilidade do NEDB com os procedimentos

[2] MILREP – Military Representative, representam o Ministro da defesa de cada nação nas reuniões.

NATO assegurando a estandardização e procedimentos, fazendo revisão da documentação e dos manuais técnicos de forma a assegurar a fiabilidade e distribuição dos dados (STANAG 6009, 2011).

- **NEWWG** – *NATO Electronic Warfare Working Group*, têm como missão principal o apoio nos plenários do NEWAC respeitante à preparação de recomendações e ao desenvolvimento dos conceitos e doutrina de EW. A validação dos conceitos EW nas publicações de doutrina NATO também faz parte das suas competências (Nieto, 2016).
- **JEWCS** – *Joint Electronic Wafare Core Staff* proporciona aos comandos e nações NATO todo o apoio e experiência no treino EW, tanto ao nível tático, operacional e estratégico. É o único órgão NATO com meios técnicos e humanos para suporte em exercícios e operações no âmbito EW conforme ilustrado na figura 3 (SHAPE, 2021, 06 de abril).

Como exemplo do que atrás foi dito, relativamente ao treino nesta área, o exercício *Naval Electro Magnetic Operations* (NEMO), realizado no fim do mês de outubro de 2019, no Reino Unido e que contou com a presença de 13 países da NATO entre eles uma unidade naval portuguesa, a saber, o NRP D. Francisco de Almeida, teve como objetivo principal o treino relativo às ameaças dos misseis hipersónicos, tendo sido simuladas defesas navais antiaéreas, clarificando qual o estado da arte relativo às defesas eletrónicas neste ambiente (NATO, 2019). A nível nacional, anualmente, realiza-se um exercício em que participam os três ramos das FFAA, que é o *Real Thaw* e que conta com os meios do JEWCS para simular vários tipos de ameaças nos três vetores ambientais (naval, terrestre e aéreo).

Figura 3 - NATO JEWCS EW Assets

Fonte: Disponível em https://ac.nato.int/archive/2017/exercise-ramstein-guard-integrates-into-dutchled-frisian-flag.

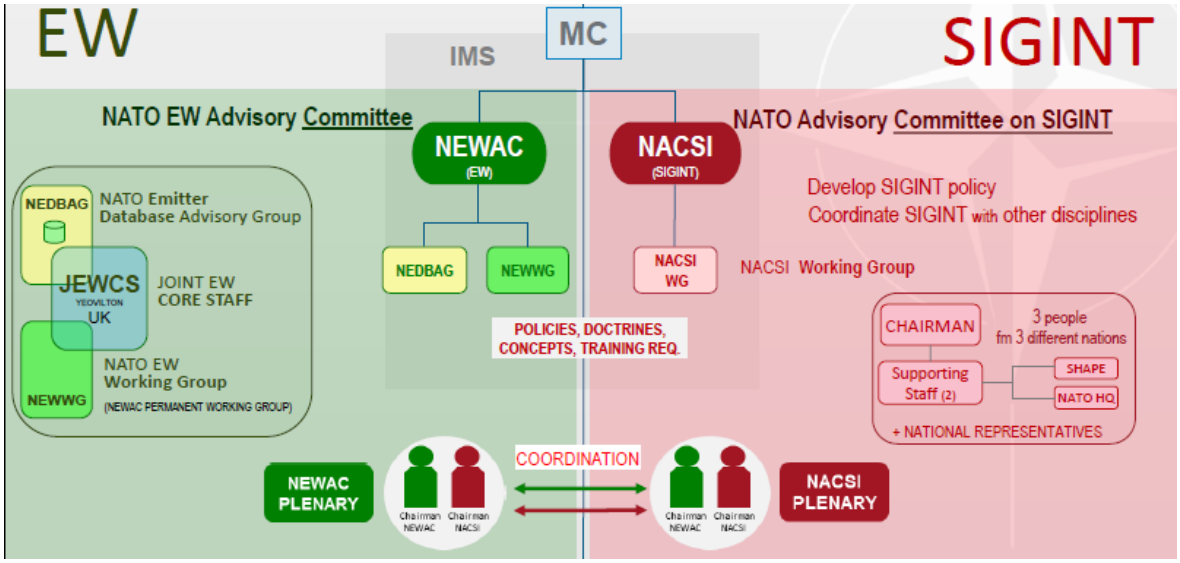

Figura 4 - Organização SIGINT e EW na NATO

Fonte: Nieto (2016).

Em 2010, foi tomada a decisão de conduzir uma reforma na Estrutura de Comando da NATO. Esta reforma foi realizada no âmbito do desenvolvimento para o Conceito Estratégico 2010, concentrando-se no esforço de garantir que a Aliança possa enfrentar os desafios de segurança do século XXI com eficácia e eficiência. A estrutura de comando é voltada para o futuro e ao ser flexível e despida de burocracia, torna-se mais acessível a todas as nações. Em comparação com as estruturas anteriores, fornece uma capacidade de C2 multinacional real implantável no nível operacional. Também oferece uma estrutura mais coerente que será compreendida por outras organizações e parceiros internacionais (NATO, 2021, 06 de abril).

Depois de décadas de negligência com a EW por parte da NATO, enquanto a Rússia e a China avançavam a passos largos nesta área, esta organização viu-se obrigada a rever a sua estratégia não só em EW, mas também na componente SIGINT devido à rápida evolução tecnológica que afeta estas duas áreas, necessitando de uma permanente atualização dos meios ao seu dispor (NATO, 2019). As forças NATO estão obrigadas a operar num EME cada vez mais complexo onde os comandos necessitam de obter a superioridade necessária relativa a este ambiente, para permitir o uso eficaz do EEM pelas forças amigas e ao mesmo tempo, utilizando este mesmo meio, explorar, prevenir ou reduzir o uso eficaz do EME por parte do inimigo. O ambiente eletromagnético é visto como um ambiente operacional, e por lá ocorrem muitas batalhas sendo considerado por muitos como um cérebro por onde circula toda a informação, e quem o dominar é capaz de derrotar o inimigo através da superioridade da informação. Não podemos esquecer que tanto a SIGINT como a EW negam, contra-atacam e neutralizam, simultaneamente todo o EEM ao adversário na área das operações (Spreckelsen, 2019). Apesar do nosso estudo estar vocacionado para a organização e capacidades de SIGINT e de EW, há um *branch* que não pode ficar de fora deste ambiente: Cyberspace – esta componente também faz parte integrante do EME operando em conjunto com as disciplinas de EW. Algumas nações NATO já reconheceram a importância de associar a Cyber às atividades EW criando o conceito CEMA[3] (*Cyber-Electromagnetic Activities*) em que congrega todas as áreas que utilizam o EEM, centralizando e canalizando toda a informação para um Centro de Operações único, no Teatro de Operações (TO), ganhando desta forma em todos os domínios quer físicos (mar, terra, ar e espaço), quer nos não-físicos (Intel, Cyber e EM) (Willis, 2020).

[3] CEMA foi criado pelo exército americano com o intuito de centralizar toda a informação relacionada com o ambiente cyber, EW, Intelligence num único Comando Tático da Operação

Figura 5 - Centro operações conjunto

Fonte: Disponível em https://projectredhand.wordpress.com/category/network-centric-warfare/

2.1. Síntese conclusiva

Pelo que atrás foi descrito, tanto a NATO como as nações aliadas, muito recentemente é que começaram a olhar com outros olhos para as questões do EME, sabendo que os conflitos futuros serão travados num ambiente cheio de tecnologia sendo para isso necessária uma reformulação quanto às questões de organização, equipamentos e interoperabilidade dos meios ao seu dispor.

Uma vez que o EEM ultrapassa todos os domínios físicos assim como as informações que lá correm, pelo que as operações conjuntas no mesmo espaço eletromagnético devem ser integradas na componente marítima, terrestre e aérea, assim como na espacial e ciberespaço, sabendo quem são as nações e quais os seus meios que equipam as forças NATO. A interoperabilidade e a congregação de recursos tornam-se cada vez mais uma prioridade quer na formação, doutrina e treino das forças NATO, sendo necessário a validação deste conceito CEMA, juntamente com uma constante atualização dos meios empregues nos TO.

Pelo que ficou referido neste capítulo, concretizou-se deste modo o OE1, assim como respondida a QD1.

3. Estrutura SIGINT e EW dos países considerados para o estudo de caso

Neste capítulo iremos debruçar sobre a estrutura e a capacidade SIGINT e EW de dois países, tendo-se optado por nações que possuem estratégias completas e mais avançadas em relação a outras pelo que estão na linha da frente relativamente à adaptação e na rápida evolução das ameaças. Sendo esta uma área em que muita doutrina é classificada, convém realçar que a investigação deste tema, foi através de doutrina e *sites* NATO classificados e através de troca de e-mails com militares e civis que prestam serviço nesta área, uma vez que em fontes abertas existe muita pouca informação, no entanto tudo o que está descrito ao longo deste trabalho não carece de classificação.

Os países escolhidos foram os Estados Unidos da América, pela sua experiência e organização, sendo uma superpotência a nível militar e que está sempre na linha da frente nos TO, obrigando por isso a manter-se sempre atualizada. A outra nação é a Alemanha que aos poucos está-se a afirmar-se com a maior potência militar na Europa, muito pelo seu passado militar e aproveitando as lições aprendidas com ele, mas também por se encontrar a modernizar as suas FFAA e consequentemente vê-se obrigada a atualizar os seus conceitos assim como a sua organização interna na interligação dos seus meios militares.

3.1. Estados Unidos da América

Como é de fácil compreensão, qualquer estrutura militar americana que seja objeto de estudo torna-se difícil de descrever e/ou interligá-la, fato pelo qual a organização ao nível da SIGINT e EW nos Estados Unidos da América (USA), não é de todo fácil. O Departamento de estado da Defesa (DoD – Department of Defense) é o maior comando governamental da América, e tem como objetivo empenhar as forças militares, em número suficiente, para travar os conflitos e garantir a segurança da nação (Department of Defense, 2021, 15 de abril). A sua estrutura, entre outros departamentos, é composta pelos três ramos das forças armadas e pelos comandos de defesa, onde se destacam os seguintes:

- *National Security Agency* (NSA) – tem como missão a gestão e validação dos aspetos relacionados com SIGINT e Cyber, com o objetivo da supremacia da informação quer nacional quer das nações aliadas. Os produtos de INTEL que produzem não são apenas virados para o consumo interno, mas também para outras nações sendo contributos valiosos na exploração do EEM. Essa informação também é disponibilizada para alguns fabricantes de equipamentos EW e utilizado na sua conceção e/ou evolução (Bernard, 2009). A NSA disponibiliza à NATO uma variedade de

relatórios e respostas aos RFI's, assim como dados de ELINT, fornecendo também informações sobre o contraterrorismo (National Security Agency, 2021, 15 de abril).

Na figura seguinte está o organograma da NSA e onde se encontra realçada a estrutura interna com interesse para este estudo e que foi referida.

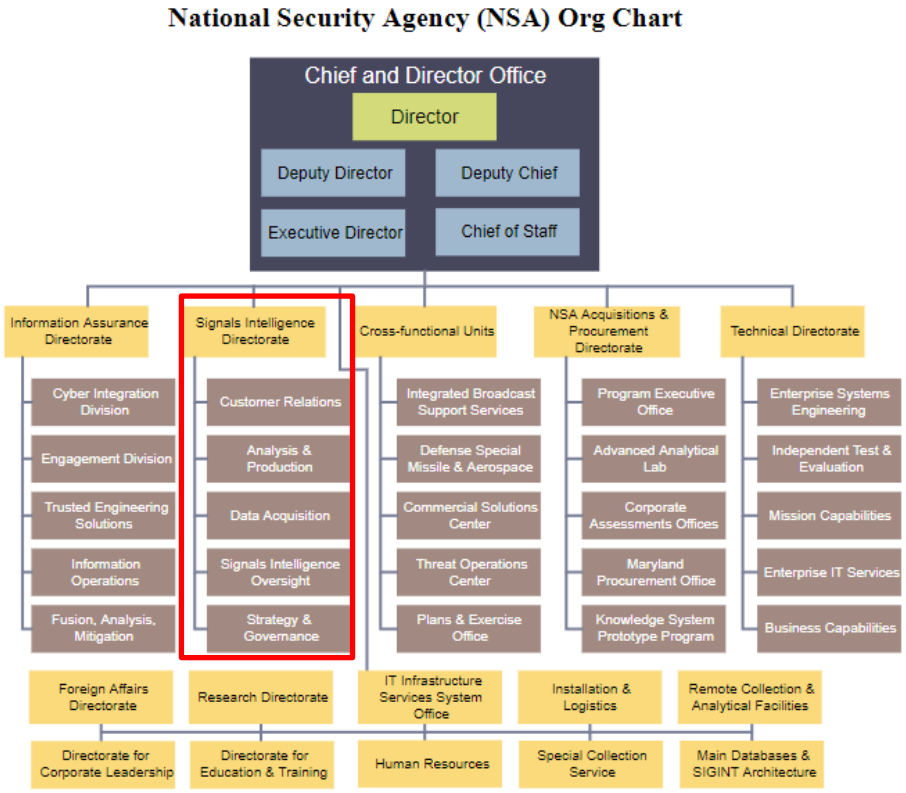

Figura 6 - Organograma da NSA

Fonte: Disponível em https://www.orgcharting.com/nsa-org-chart/

- *Defense Information Systems Agency* (DISA) - é um centro de excelência do DoD para aspetos relacionados com o EEM. Uma das suas missões é fornecer informações do *Electromagnetic Enviromental Effects* (E3) de modo que os equipamentos funcionem sem limitações neste ambiente eletromagnético, para isso contam com um departamento dedicado a esse fim que é o *Defense Spectrum Organization* (DSO). O apoio da engenharia torna-se fundamental nas operações que utilizam o espetro eletromagnético como campo de batalha. Em ambientes operacionais futuros, é vital que os sistemas funcionem como o esperado para atingir os objetivos da missão (Harris, 2016). As forças armadas norte-americanas reconhecem que o

sucesso de uma missão depende da coordenação conjunta do espectro o que para isso requer uma adaptação dos procedimentos militares, bem como dos equipamentos, uma vez que o EEM está cada vez mais congestionado e as operações conjuntas incluem atividades de EW para explorar, atacar, proteger e gerir todo o espetro. Por outro lado, os equipamentos utilizados nas operações de defesa podem causar e/ou serem afetados pela interferência no espetro eletromagnético (Harris, 2016). Neste caso concreto a DISA em estreita colaboração com a DSO visam garantir que a distribuição desse mesmo espetro não conflitue com a utilização dos equipamentos no EME, porque essa mesma interferência pode ser causada pelo adversário ou pela falta de coordenação entre forças amigas, sendo para isso necessário melhorar a eficácia dos equipamentos para que possam operar conforme pretendido em ambientes congestionados, ou como é conhecido por *Electromagnetic Battlefield* (Sharpe, 2018).

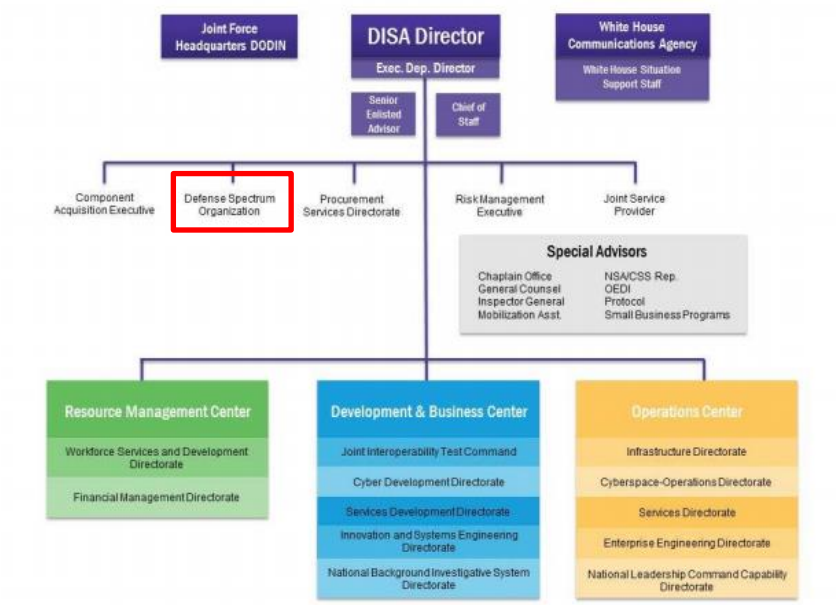

Figura 7 - Organograma da DISA

Fonte: Disponível em https://comptroller.defense.gov/Portals/45/Documents/afr/fy2018/DoD_Components/2018-AFR-DISA-GF.pdf

- *Defense Intelligence Agency* (DIA) – centro de INTEL que fornece informações relevantes sobre as forças armadas estrangeiras a todas as unidades militares e agências do estado norte-americano para apoio ao planeamento de operações militares assim como na aquisição de sistemas de armas (Knight, 2003).

Na figura seguinte destacam-se as três agências que acabámos de referir e que estão inseridas no organograma do Secretário de Defesa norte-americano.

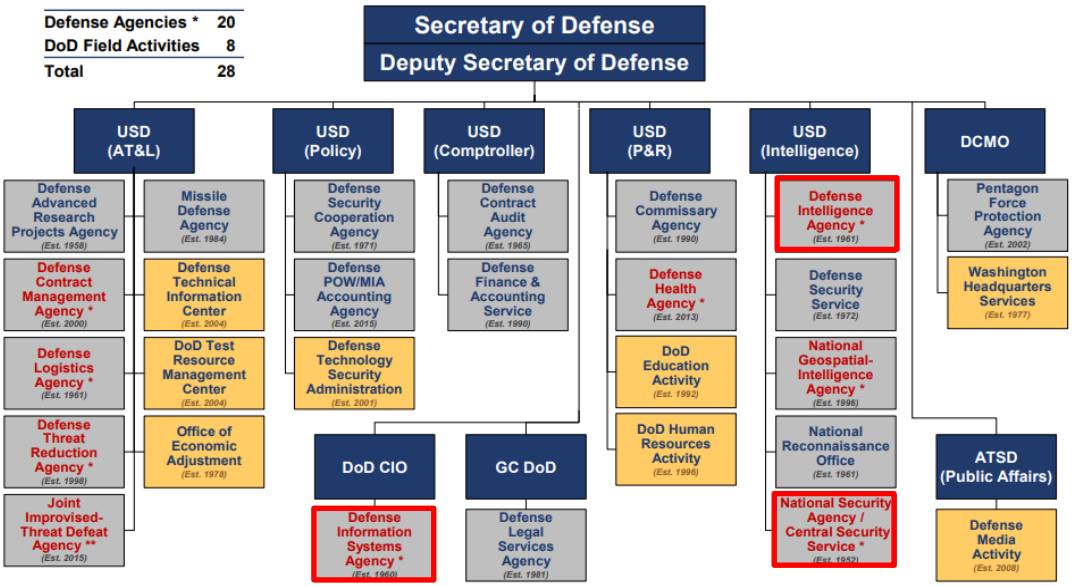

Figura 8 - Organograma das agências de defesa

Fonte: Disponível em https://cmo.defense.gov/Portals/47/Documents/OSD%20DAFA%20Organization.pdf

Em suma todos necessitam de aceder ao EEM, sejam agências governamentais, sejam forças militares ou até mesmo o comum do civil. Nós estamos dependentes do que se passa neste ambiente para comunicarmos, para aceder à internet, ouvir música ou utilizar outros recursos como o *wireless*, mas como fazemos a gestão deste espaço no seio militar, ou melhor, como fazem as nações com as valências como é o caso da norte-americana? Como diz Willis (2020): "*Our ability to master this increasingly complex and congested environment will be critical to achieving and sustaining advantage over our adversaries. To do so we must pay attention to how we provide and orchestrate our Cyber and Electromagnetic Activity (CEMA).*" O CEMA consiste nas *Cyberspace Operations* (CO), EW e *Spectrum Management Operations* (SMO). Apesar do modo de as empregar divergirem, as funções e capacidades devem ser integradas por forma a garantir sinergias entre si e obter a supremacia no EEM (FM 3-38, 2014).

3.2. Alemanha

Relativamente ao conceito adotado pelas forças armadas alemãs, na sua doutrina a Cyber e a INTEL estão no topo sob a tutela do Ministro da Defesa, garantindo assim a autonomia e a proteção do estado. Este comando de Cyber e INTEL (*Kommando Cyber- und Informationsraum*) é o que foi criado há menos tempo na estrutura militar alemã e tem como missão a segurança da informação. Na sua estrutura, encontra-se o Comando de

Reconhecimento Estratégico que tem como objetivo recolher e analisar as informações para fornecer aos tomadores de decisão informações válidas em tempo útil para sucesso da missão. Neste comando as capacidades de SIGINT, EW, Cyber e INTEL estão todas interligadas, como demonstra a fig.9., onde as informações obtidas depois de tratadas e analisadas, são elaborados relatórios, tendo como função principal empenhar as forças militares, em número suficiente, para travar os conflitos e garantir a segurança da nação. Existe ainda um Centro de IMINT que dá apoio às FFAA nas operações, recolhendo imagens satélite, analisando e produzindo produtos de IMINT para que as forças no terreno tenham um conhecimento real do que vão encontrar (i.e., aeroportos, pontos de evacuação, infraestruturas críticas, posicionamento das forças opositoras assim como as suas capacidades militares) (Bundeswehr, 2021, 23 de maio).

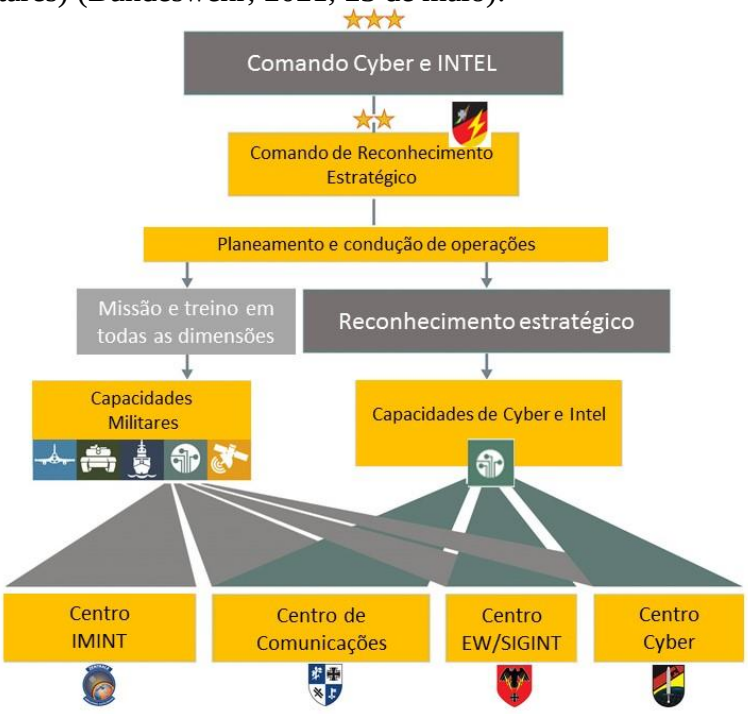

Figura 9 - Organograma do Comando Cyber e INTEL das FFAA alemãs

Fonte: Disponível em https://www.bundeswehr.de/de/

3.3. Síntese conclusiva

Como descrito neste capítulo, estas duas nações encontram-se na vanguarda a nível de conhecimento e de organização pelo que utilizam os sistemas das suas FFAA para a recolha de informação. Depois de recolhidos são enviados para um centro que faz a análise e validação desses mesmos dados para a produção dos produtos de INTEL, concentrando assim toda a informação num mesmo local e disponibilizando-a quem dela necessita.

Deste modo fica concretizado o OE2 assim como respondida a QD2.

4. Estrutura SIGINT e EW nas FFAA

Neste capítulo iremos abordar a estrutura e a capacidade SIGINT e EW nas nossas FFAA.

Os ramos têm vindo a adaptar-se na medida do possível, às suas necessidades por um lado e por outro tendo em conta o que é requisito quando operam em forças conjuntas, para uma integração plena nas capacidades e requisitos operacionais dos TO onde operam. Assim passarei a descrever qual a organização de cada ramo, tendo como base as entrevistas semiestruturadas efetuadas aos experts de cada ramo e com base nos seus inputs irei referir quais os equipamentos existentes e quais os que estão a ser modernizados ou em vistas de aquisição por forma a reequipar os ramos nesta componente.

4.1. Marinha

Na Marinha a entidade responsável pela análise e validação dos dados paramétricos, assim como todo o processo de carregamento dos sistemas de combate das unidades que possuem capacidade de ELINT, COMINT e ACINT é o Centro de Gestão e Análise de Dados Operacionais (CADOP) que viu o seu regulamento interno recentemente aprovado pelo Despacho do Almirante Chefe do Estado-Maior da Armada n.º 25/2020, de 13 de maio, onde está identificada a sua competência para exercer as funções de Signals Intelligence (SIGINT) e SIGINT Electronic Warfare Operations Centre (SEWOC) da Marinha.

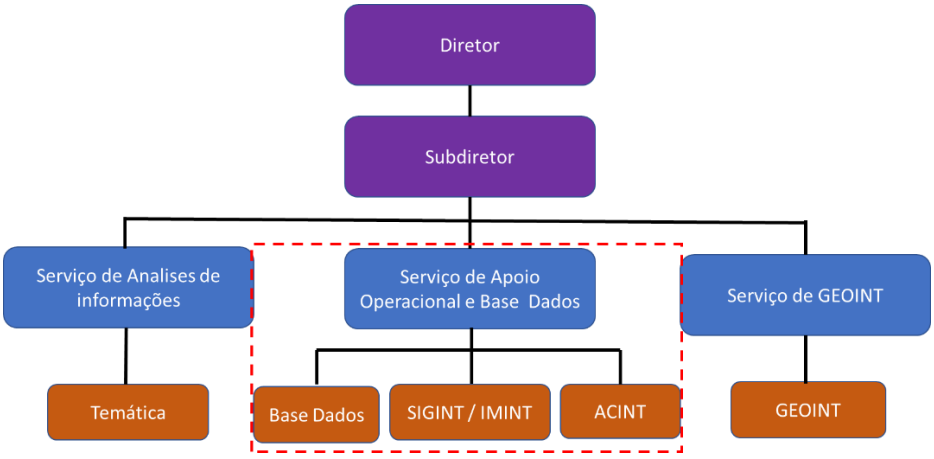

Figura 10 - Organograma do CADOP

(https://intranet.marinha.pt/subportais/CN/CADOP/Paginas/Organiza%C3%A7%C3%A3o.aspx)

De acordo com o Despacho do Almirante CEMA nº42/10, de 6 de maio, o CADOP tem por missão:

"*Assegurar aos Comandos e às Forças e Unidades em operações, o apoio necessário à gestão da informação e do conhecimento, no âmbito da superioridade de informação e de decisão.*"

É neste Centro que se concentra toda a informação paramétrica recolhida pelas unidades navais de superfície e subsuperfície, que depois de analisadas são colocadas numa base de dados designada por Sistema de Gestão Integrado de Dados Operacionais (SIGIDOP). Aqui encontram-se os dados recolhidos pelas nossas fragatas e submarinos e também a BD da NATO - NEDB, que serve como suporte a toda a informação (Baptista, 2021). Esta ferramenta também tem a possibilidade de armazenar a informação paramétrica, depois de analisada e validada, que tenha sido enviada pela FAP.

As capacidades que a Marinha possui na área de SIGINT e EW é a que se encontra representada no seguinte quadro:

Quadro 3 - Sistemas de SIGINT e EW na Marinha

Unidades Navais	EW		COMINT
	ESM	ECM	
Vasco da Gama	SIM	SIM	NÃO
Alvares Cabral	SIM	SIM	NÃO
Corte Real	SIM	SIM	NÃO
Bartolomeu Dias	SIM	SIM	NÃO
D. Francisco de Almeida	SIM	SIM	NÃO
Tridente	SIM	NÃO	SIM
Arpão	SIM	NÃO	SIM

À presente data encontra-se a decorrer o processo de modernização nas duas fragatas classe Bartolomeu Dias, pelo que estas unidades vão ficar equipadas com um novo sistema de EW, assim como pela primeira vez Portugal passa a contar com um equipamento de eletro-óticos nas suas unidades de superfície. Por outro lado, a Marinha deixa cair por completo a capacidade ativa de EW (ECM), ficando apenas com a componente passiva (ESM) (Baptista, 2021).

Relativamente à representação da Marinha Portuguesa no seio do NEDBAG, cabe ao CADOP garantir a representação neste fórum desde que associados às bases de dados de SIGINT (CEMA, 2020).

Na MAR não existe nenhum exercício dedicado à componente EW, pelo que na base de oportunidade nos exercícios nacionais (e.g. INSTREX, CONTEX, SWORDFISH) tenta-se inserir séries dedicadas ao treino dos operadores, mas por diversas razões estas séries não são realizadas sendo muita das vezes canceladas (Baptista, 2021). O único exercício que a MAR participa e que fornece algum realismo, sempre que o JEWCS integra o mesmo, é o Real Thaw (RT), uma vez que os *assets* do JEWCS que estão envolvidos neste exercício permitem simular vários radares de superfície. A plataforma aérea DA-20 pode equipar, a

pedido, vários simuladores de empastelamento permitindo assim a simulação de vários tipos de misseis ou outras ameaças aéreas. De referir ainda que o RT é um exercício conduzido pela FAP, pelo que a MAR é convidada a integrá-lo (Baptista, 2021).

A nível internacional, o último exercício dedicado à EW organizado pela NATO e que contou com a presença de uma unidade naval portuguesa, a saber o NRP D. Francisco de Almeida, foi em 2019 tendo decorrido na costa inglesa. Devido a vários fatores ainda não foi possível fazer uma análise, nem uma leitura atenta ao relatório gerado no fim do exercício (Baptista, 2021). Tal fato invalidou que pudesse ser incluído neste trabalho qualquer referência ao mesmo, para saber qual o estado da arte a nível internacional.

4.2. Exército

No caso da EW no Exército, a unidade responsável por esta área é a Companhia de Guerra Eletrónica (CompGE) em que a sua missão passa por garantir a superioridade de informação, através das operações EW, sendo composta pelos seguintes pelotões:

- Pelotão de Guerra Eletrónica médio, constituído por três secções: i) MAE – Medidas de apoio eletromagnéticas; ii) CME – Contra medidas eletromagnéticas; iii) GEUrb – Guerra Eletrónica Urbana.
- Pelotão de Guerra Eletrónica ligeiro, constituído por três secções: i) VigEletr – Vigilância Eletromagnética; ii) AtEletr – Ataque Eletromagnético; iii) DefEletr – Defesa Eletromagnética.

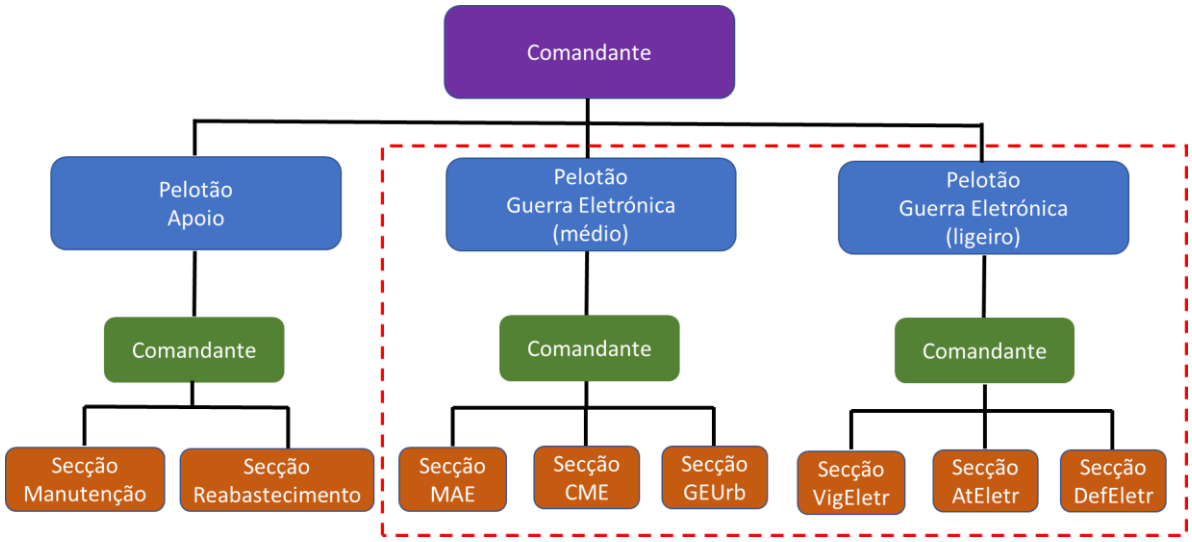

Figura 11 - Organograma da Companhia GE

Fonte: Capitão Costa (2021)

O treino contra sistemas de defesa aérea, por exemplo, é da responsabilidade do EXE, mas devido à falta de investimento, estes equipamentos estão desatualizados e em alguns

casos inoperativos. Apesar de a EW ser apresentada como de uma realidade se tratasse e pese embora no que está a ser investido nesta área, o fato é que ainda está a ser criada esta capacidade, assim como a definição para a sua missão, quais as suas competências e como será inserida na estrutura do EXE (Costa, 2021). Nesta perspetiva, pretende-se criar um centro de Guerra Eletrónica de excelência para o EXE, que desempenhe um papel relevante na obtenção de informação, na análise/catalogação, no processamento e na disseminação para que possa assumir um papel de destaque na componente de informações o que atualmente não se verifica, muito embora o esforço que se vem realizando desde 2018, com a identificação das necessidades, quer a nível de infraestruturas C2, quer a nível de sistemas, pelo que poder-se-á considerar como o primeiro passo desta reestruturação a formação em EW, realizada em 2020, contando também com a participação e a partilha de conhecimento dos outros dois ramos das FFAA (Costa, 2021).

A nível de representação do EXE no grupo NATO, para a SIGINT/EW e como ainda não foi criado um regulamento interno que caracterize e identifique quem tem a incumbência de participar, tem sido um pouco *ad-hoc* a presença do Cap. Costa nestas reuniões e no acesso à informação nela contida, assim como na partilha dos dados relativamente ao NEDB (Costa, 2021).

Uma vez que os sistemas estavam a entrar em obsolescência e sendo o foco do EXE para a SIGINT, poder voltar a contar com esta capacidade, estando a decorrer o processo de reedificação prevista no âmbito da Lei da Programação Militar até 2023, a CompGE foi recentemente reequipada com sistemas táticos de ESM focados nas bandas V/UHF de comunicações[4], prevendo-se também a aquisição de equipamento de nível operacional focados em CESM (H/V/UHF e WIFI/mobile ESM), CECM (H/V/UHF e WIFI/mobile ESM), C-UAS (NATO CLASS I e II)[5]. Por ultimo está a ser pensado a rearticulação do Quadro Orgânico da CompGE no sentido de agilizar o processo de apoio a unidade de escalão abaixo de Brigada, ou seja, em vez de empenhar a CompGE como um todo, serão articuladas Equipas Destacáveis de EW (EDGE) por forma a gerar forças "*mission taylored*" que mais não é do que diferentes configurações que pode ir desde um elemento de EW até à própria companhia, dependendo da missão atribuída, com o intuito de um esclarecimento completo do TO e consequentemente a proteção da força para o sucesso da missão. Sendo

[4] os equipamentos recentemente adquiridos estão em processo de credenciação pelo que a divulgação da sua identificação, quantidade e conceito de emprego se torna sensível

[5] os processos de aquisição estão em fase de elaboração e aprovação do nível político e todos estes processos estão, à data classificados como CONFIDENCIAL

as EDGE um conceito inovador nas nossas FFAA, e neste caso particular no EXE, a formação (complexa e exigente) assim como o treino que os operadores de EW vão necessitar, torna-se num *handicap* para a sua aplicabilidade a curto prazo, mas que está a ser trabalhada para ser uma realidade a médio prazo (Costa, 2021).

4.3. Força Aérea

Na Força Aérea Portuguesa, a entidade responsável pelo apoio às esquadras no âmbito da EW é o Centro de Guerra Eletrónica (CGE) e que tem a seguinte composição:

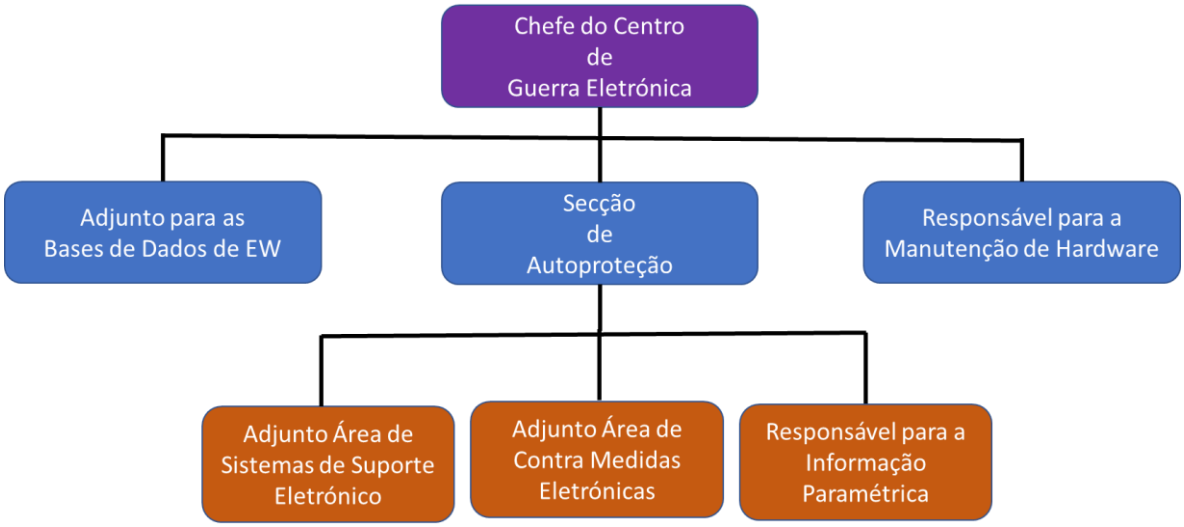

Figura 12 - Organograma do Centro de Guerra Eletrónica

Fonte: Maj. Freitas (2021)

A missão deste Centro e de acordo com o MCLAFA 305-4[6] é o de "*Apoiar a exploração dos sistemas de Guerra Eletrónica dos diversos Sistemas de Armas na Força Aérea.*".

Como tal é aqui que a programação dos sistemas das aeronaves, baseado nas bases de dados nacional (pertencente à FAP) e da NATO – NEDB é feita (Freitas, 2021). As BD são uma ferramenta primordial para o sucesso de uma missão, porque se não soubermos quem está ao nosso redor, nem quais os tipos de ameaça que representam para a nossa força, toda a missão fica comprometida, daí ser necessário um gabinete onde os analistas possam fazer a extração das gravações e analisá-las para serem carregues numa BD de forma que na próxima missão os equipamentos estejam atualizados com as ultimas recolhas paramétricas, aumentando assim o grau de fiabilidade nas suas interceções (Freitas, 2021).

Tal como nos outro ramos das FFAA, é deste centro que saí o responsável pela representação nacional (ao nível da capacidade aérea) no NEDBAG, com a tarefa de

[6] MCLAFA 305-4: Manual de Organização e Normas de Funcionamento da Direção de Engenharia e Programas

atualizar o NEDB na sua área especifica, assim como na disseminação, uma vez que esta ferramenta é a base para a programação dos sistemas da FAP.

Como referido no paragrafo da MAR, a Força Aérea sofre do mesmo problema relativamente aos exercícios dedicados de EW, uma vez que são escassos ou inexistentes. Aqui, tal como atrás referido, o RT torna-se no evento com maior protagonismo para treino das esquadras e dos operadores EW, sem ele esta capacidade vai perdendo as suas valências. Por vezes recorrem-se a EW *trials* com a Marinha Portuguesa, sempre que esta coloca uma unidade naval no mar devido à necessidade também ela de treinar os seus operadores, mas não fazendo desta missão um exercício dedicado à componente EW, mas sim na base da oportunidade fazer com que os equipamentos e os operadores sejam testados. Quando tal acontece o CGE e o CADOP reúnem-se para elaborar um caderno de treino por forma a rentabilizar ao máximo estas pequenas oportunidades de exploração dos sistemas EW de ambos os ramos (Freitas, 2021).

As capacidades EW atuais da FAP são as que se encontram no seguinte quadro:

Quadro 4 - Sistemas de EW na Força Aérea

Plataformas Aéreas	EW	
	ESM	ECM
C-130H	SIM	SIM
C-295M	SIM	SIM
EH-101	SIM	SIM
F-16MLU	SIM	SIM
P-3C CUP+	SIM	SIM

Na sua entrevista, o Major Freitas referiu ainda que: “o treino EW é muito limitado ou até mesmo inexistente, pelo que as esquadras necessitam rapidamente de efetuar novos voos para reerguer esta capacidade. Se ao treino associarmos o envelhecimento dos sistemas, então poderemos dizer que precisamos urgentemente de alertar as chefias para o estado da arte na FAP”. Sobre o futuro da EW na FAP o Major Freitas revelou estar em curso a aquisição de uma nova plataforma para substituir o C-130H e com ela associado um novo equipamento EW, assim como um simulador e equipamento de analise de sinais para dotar o CGE com esta valência (Freitas, 2021).

5. Conclusão

Neste trabalho de investigação foi aplicada uma estratégia de investigação qualitativa centrada na análise documental e em entrevistas semiestruturadas a elementos-chave dos três ramos das FFAA, que detêm a responsabilidade na programação dos sistemas SIGINT/EW a nível nacional assim como na análise dos dados recolhidos pelos equipamentos, validação e submissão para as diferentes BD. São eles também os representantes nacionais nas reuniões da NATO relativas às Base de Dados (NEDB). Para este estudo foram também utilizadas as ferramentas de fontes abertas para validar a maneira de atuar das organizações congéneres, assim como ferramentas classificadas da NATO.

Tendo sempre como foco o problema concreto, que passa por uma inexistência na gestão de operações conjuntas na congregação das sinergias para obtenção do sucesso da missão, o Objetivo Geral (OG) desta investigação consistiu na análise de arquitetura de interoperabilidade de SIGINT e de EW ao nível militar conjunto, pelo que o capítulo 2 serviu para responder à QD1: "Como se caracterizam as estruturas de SIGINT e EW na NATO?" e o capítulo subsequente visou responder à QD2: "Como se caracterizam as estruturas de SIGINT e EW dos Estados Unidos da América e da Alemanha?". Por fim, no capítulo 4 ficou respondida a QD3: "Como se caracterizam as estruturas de SIGINT e EW nos três ramos das FFAA?", pelo que a resposta ao OG "ANALISAR possíveis caminhos de implementação de arquitetura de interoperabilidade de SIGINT e de EW ao nível militar conjunto." será desenvolvido nos próximos parágrafos.

Durante a realização deste trabalho, verificou-se que a área SIGINT e EW teve um interregno desde o fim da Guerra Fria até ao 11 de setembro 2001, altura em que as nações despertaram para uma nova realidade e começaram a desenvolver sinergias para colmatar esse interregno, ao passo que nações não-NATO como a Rússia e a China, nunca pararam no desenvolvimento e modernização desta capacidade. Foi com base nessa evolução que algumas nações NATO começaram a reorganizar e a desenvolver novas formas de lutar contra aquilo que hoje falamos e caracterizamos como a Cyber warfare associado ao SIGINT e à EW, ou como alguns autores identificam e já aqui retratado o CEMA. A maioria dos países tem feito um forte investimento quer na aquisição de equipamentos, quer na reestruturação das suas organizações assim como no treino. Como ficou demonstrado neste trabalho os Estados Unidos e a Alemanha, apesar de terem uma organização diferente relativamente ao nível do SIGINT e da EW, a base é a mesma, ou seja, as Forças Armadas têm os equipamentos e os operadores especializados, são eles que estão no terreno a recolher

toda a informação, que depois será alvo de tratamento, analise e validação para posterior disseminação. Esta última parte é feita por analistas especializados e dedicados a esta área em bases militares ou em edifícios dos quartéis-generais das FFAA. Por outro lado, em Portugal, verifica-se que o investimento na componente SIGINT e EW continua a ser uma miragem pelo que as plataformas e sistemas estão na sua obsolescência e o treino e operadores especializados não existem. Ao nível de analistas nesta área, constatou-se serem militares que estão colocados nos Centros de SIGINT e EW, que ora encontram-se naqueles locais ora são destacados para outras unidades desempenhando funções que nada tem a ver com a SIGINT/EW, perdendo-se deste modo todo o conhecimento adquirido assim como a experiência e valor agregado. Este trabalho serviu também para identificar que cada ramo possui uma Base de Dados própria e não partilhada com os outros ramos. Apesar da existência de protocolos entre ramos (como é o caso da MAR e da FAP) o mesmo só é utilizado quando as unidades navais ou plataformas aéreas deslocam-se para um determinado TO e não existe informação suficiente sobre o mesmo.

Pelo que aqui foi dito propõem-se a criação de uma unidade de SIGINT e de EW no EMGFA, composta por militares dos três ramos e por analistas especializados e dedicados apenas a esta área e em estreita colaboração com a capacidade de Cyber que está a ser edificada também no EMGFA. Este comando seria composto por três secções (Missão e Treino, Componente Técnica e Componente Operacional) em que a:

- **Missão e Treino** – Responsável pela ligação entre as os ramos e o EMGFA na recolha da informação das plataformas nacionais e disseminação das EOB aquando das atribuições das missões aos Centros EW dos respetivos ramos para a programação dos sistemas de bordo das plataformas. Seriam também responsáveis pela criação de exercícios conjuntos por forma a validar as TTP e para as unidades não perderem as valências nesta área. Teriam também responsabilidade pela informação recolhida e certificando se os equipamentos estão operacionais ou a necessitar de algum tipo de intervenção/calibração, antevendo desta forma percalços futuros na degradação dos sistemas.
- **Componente Técnica** – Encarregue pela manutenção e validação dos requisitos técnicos da Base de Dados Nacional (BDN) e representante nacional no NEDBAG, sendo o responsável pela atualização do NEDB a nível nacional.
- **Componente Operacional** – Nesta secção ficam os analistas com a responsabilidade de analisar e de validarem os dados recolhidos pelas

diferentes plataformas nacionais, dos três ramos das FFAA e depois submeterem na BDN, encontrando-se divididos pelas seguintes áreas:

- **GEOINT**
- **SIGINT/EW**
- **ACINT**
- **IMINT**

O quadro orgânico geral teria o seguinte aspeto:

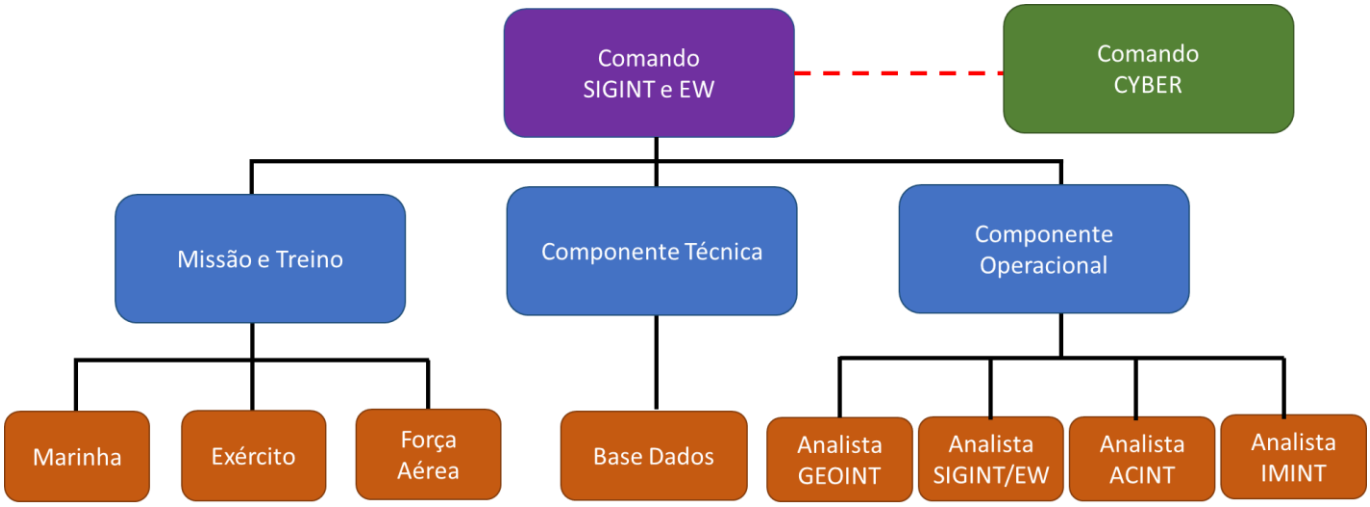

Figura 13 - Organograma do Comando SIGINT/EW proposto

(Fonte: Autor, 2021)

A tracejado encontra-se uma ligação funcional com o Comando Cyber, para partilha de informação a nível desta componente sobre o TO em que as FFAA fossem destacadas.

A Secção de Missão e Treino poderia ficar sobre o comando operacional do Comando Conjunto para as Operações Militares (CCOM), enquanto as Secções da Componente Técnica e da Operacional sobre a responsabilidade da Direção de Comunicações e Sistemas de Informação (DIRCSI).

Quanto à formação necessária, principalmente para os analistas da Secção da Componente Operacional, nas diferentes áreas funcionais, ficaria numa primeira fase pelo o que atualmente existe nos ramos, aproveitando desta forma toda a experiência e o *know-how* dos mesmos, procedendo-se ao seu movimento das unidades onde prestam serviço para esta nova estrutura do EMGFA, procedendo-se paralelamente ao incremento dos efetivos nos diferentes sectores, por forma a aumentar o numero de analistas aproveitando a esperiência dos que estariam já integrados numa primeira fase e com esta oportunidade ganhar-se-ia tempo para dar-lhes as formações necessárias para o desempenho das suas funções conforme *Job Description* a ser definido.

Sabendo que a BD utilizada na Marinha, o SIGIDOP, recebe vários tipos de informação vinda de diferentes fontes e em formatos distintos (i.e. .csv, .xml, .mdb, .jpg), mas reconhecida pelo SIGIDOP como é o caso do NEDB, dados da FAP, Imagens, dados Georreferenciados e dados de ELINT, COMINT e ACINT, estes últimos recebidos das unidades navais, poderia servir para testar uma solução de BDN e desta forma não incrementar custos nesta fase embrionária. Realça-se ainda que na exportação das missões consegue-se efetuar não só para as unidades navais como também para as aeronaves da FAP, tendo apenas o CGE da FAP, efetuar a conversão do *software* para ser lido nos sistemas de bordo.

Por fim, julga-se especialmente relevante o desenvolvimento de trabalhos futuros nesta área, aproveitando o trabalho já desenvolvido, caso este modelo venha a ser implementado, para validar a sua eficácia e eficiência ou outros pontos a corrigir e assim prosseguir com o que foi definido no desenho de pesquisa no capítulo 1 sobre a *Grounded Therory* e assim criar uma nova tipologia de organização de SIGINT e EW para ser testada e validada.

Referências Bibliográficas

Agências de Defesa. (2021) Organograma das agências de defesa. Retirado de https://cmo.defense.gov/Portal/47/Documents/OSD%20DAFA%20Organization.pdf.

Bernard, R. (2009). ELINT at NSA. Retirado de https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/technology/elint.pdf?ver=2019-08-07-124409-477.

Bundeswehr. (2021, 23 de maio). Retirado de https://www.bundeswehr.de/de/.

Chefe do Estado-Maior da Armada. (2010). Despacho do Almirante Chefe do Estado-Maior da Armada nº42/10, de 6 de maio.

Chefe do Estado-Maior da Armada. (2020). Despacho do Almirante Chefe do Estado-Maior da Armada n.º 25/2020, de 13 de maio.

Cullen, M. (2014). Spectrum Management [versão PDF]. Retirado de https://www.afcea.org/events/augusta/14/documents/T3S2SpectrumManagement.pdf

Defense Information Systems Agency. (2021). Organograma [versão PDF]. Retirado de https://comptroller.defense.gov/Portals/45/Documents/afr/fy2018/DoD_Components/2018-AFR-DISA-GF.pdf.

Department of Defense. (2021, 15 de abril). Retirado de https://www.defense.gov/Our-Story/.

Dura, M. (2017). Electronic Warfare: Russian Response to the NATO's Advantage?. Retirado de https://www.defence24.com/electronic-warfare-russian-response-to-the-natos-advantage-analysis.

Estado-Maior-General das Forças Armadas. (1994). Política de Guerra Eletrónica para as Forças Armadas (PEMGFA).

FM 3-38. (2014). Cyber Electromagnetic Activities [versão PDF]. Retirado de https://fas.org/irp/doddir/army/fm3-38.pdf.

Força Aérea Portuguesa. (2012). FAP 2012a, MCLAFA 305-4 Organização e Normas e Funcionamento da Direção de Engenharia e Programas. Alfragide: CLAFA.

Harris. (2016). DSO missão. Retirado de https://govtribe.com/opportunity/federal-contract-opportunity/defense-spectrum-organization-dso-electromagnetic-spectrum-ems-services-applied-engineering-spectrum-and-e3-engineering-support-hc104715r4012.

Instituto Universitário Militar. (2021). Orientações Metodológicas para a elaboração de trabalhos de Investigação 2Ed.

Knight, J. (2003). "Defense Intelligence Agency" Encyclopedia of Espionage, Intelligence and Security.

MC 0515. (2012) Concept for the NATO SIGINT & EW Operations Centre (SEWOC).

MCM 0142. (2007). Military committee transformation concept for future NATO Electronic Warfare.

National Security Agency. (2021, 15 de abril). Retirado de https://www.nsa.gov/.

NATO. (2021, 06 de abril). Operações de Comando Aliado (ACO) em 23out2020. Retirado de https://www.nato.int/cps/en/natolive/topics_52091.htm.

NATO. (2021, 06 de abril). Retirado de https://www.nato.int/cps/en/natohq/topics_80906.htm.

NATO. (2021, 10 de junho). Retirado de https://www.nato.int/cps/en/natohq/who_is_who_51627.htm.

NEP / INV 001 (A1) (2020). Procedimentos relativos à elaboração de trabalhos de investigação realizados no âmbito de cursos que não atribuem grau académico. Lisboa: Instituto Universitário Militar.

Nieto, I. (2016). EW Overview [versão PDF]. NATO School, Oberammergau.

Presidência do Conselho de Ministros. (2021). Proposta de lei 862/XXII/2021. Proposta de alteração à Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA) [versão PDF].

SHAPE. (2021, 06 de abril). Retirado de https://shape.nato.int/page1139304/nato-joint-electronic-warfare-core-staff-jewcs.aspx.

Sharpe. (2018). UDISA/DSO missão. Retirado de https://www.afcea.org/content/improving-operations-complex-spectrum-environment.

Spreckelsen, V. (2019). The journal of the JAPCC [Página online]. Retirado de https://www.japcc.org/wp-content/uploads/JAPCC_J28_screen.

Steven, O. (2014). Electronic Warfare Portfolio [Página online]. Retirado de https://www.afcea.org/events/augusta/14/tracks.asp#ElectronicWarfare.

Turnbull, G. (JUN20). Global Defence Technology. Retirado de https://defence.nridigital.com/global_defence_technology_jun20/nato-electronic-warfare-investment.

Van Niekerk, B., & Maharaj, M. (2009). The Future Roles of Electronic Warfare in the Information Warfare Spectru.Journal of Information Warfare, 8(3), 1-13. Retrieved March 21, 2021, Retirado de https://www.jstor.org/stable/26486763.

Willis, M. (SET20). Cyber-Electromagnetic Domain - The Necessity of Integrating the Electromagnetic Spectrum's Disciplines Under a Single Domain of Operations. Retirado de https://www.japcc.org/cyber-electromagnetic-domain/.