INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2016/2017

TIG AEE

O CIBERESPAÇO COMO 5.º DOMÍNIO OPERACIONAL. IMPACTO ESTRATÉGICO NA POLÍTICA DE DEFESA NACIONAL.

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.

CMG EMT Manuel da Costa Honorato

COR TM Luís Filipe Camelo Duarte Santos

COR MED Regina Maria de Jesus Ramos Mateus

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO COMO 5.º DOMÍNIO OPERACIONAL IMPACTO ESTRATÉGICO NA POLÍTICA DE DEFESA NACIONAL

CMG EMT Manuel da Costa Honorato

COR TM Luís Filipe Camelo Duarte Santos

COR MED Regina Maria de Jesus Ramos Mateus

Trabalho de Investigação de Grupo da

Área de Ensino de Estratégia

CPOG 2016/2017

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O CIBERESPAÇO COMO 5.º DOMÍNIO OPERACIONAL IMPACTO ESTRATÉGICO NA POLÍTICA DE DEFESA NACIONAL.

CMG EMT Manuel da Costa Honorato

COR TM Luís Filipe Camelo Duarte Santos

COR MED Regina Maria de Jesus Ramos Mateus

Trabalho de Investigação de Grupo da

Área de Ensino de Estratégia

CPOG 2016/2017

Pedrouços 2017

Declaração de compromisso Antiplágio

Nós, **Manuel da Costa Honorato, Luís Filipe Camelo Duarte Santos** e **Regina Maria de Jesus Ramos Mateus,** declaramos por nossa honra que o documento intitulado **"O Ciberespaço como 5.º Domínio Operacional. Impacto estratégico na Política de Defesa Nacional."** corresponde ao resultado da investigação por nós desenvolvida enquanto auditores do **Curso de Promoção a Oficial General 2016/2017** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

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

Pedrouços, 7 de março de 2017

CMG EMT Manuel da Costa Honorato

_____

COR TM Luís Filipe Camelo Duarte Santos

_____

COR MED Regina Maria de Jesus Ramos Mateus

_____

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

A realidade atual da comunicação em rede assente num espaço global, onde circulam fluxos de informação e estão baseados a maioria dos processos de interação da atividade humana e tecnológica, propicia também a inerente conflitualidade entre os diversos atores, consubstanciando o ciberespaço como um espaço com relevantes impactos estratégicos nas políticas de defesa dos países, de que Portugal não é exceção.

Recorrendo a um processo hipotético-dedutivo, utilizando uma estratégia qualitativa e um modelo de "estudo de caso", identificaram-se as diferenças e semelhanças do ciberespaço comparativamente aos demais domínios operacionais, uma caracterização do posicionamento da OTAN e da UE, no reconhecimento do ciberespaço como domínio operacional, e por fim, procedeu-se a uma análise do impacto dessa decisão para as Forças Armadas Portuguesas.

A investigação efetuada permitiu concluir que o ciberespaço é, em quase todos os aspetos, diferente dos restantes domínios operacionais, exigindo uma abordagem estratégica própria e diferenciada, e que se torna necessário uma revisão à política de Defesa Nacional por forma a acomodar um novo enquadramento organizacional para a capacidade de ciberdefesa, reorientando o foco da segurança da informação, para o cumprimento da missão, como capacidade militar.

Palavras-chave: Ciberespaço, Ciberdefesa, Domínio Operacional, Política de Defesa Nacional

Abstract

The actual reality of network communication based on a global space, where the information flows run's and where the majority of the process and activity of human-technology interaction are based, also promote the inherent conflict between the various actors, consubstantiating the cyberspace as a space with relevant strategic impact on the nation's defence politic, of which Portugal is not an exception.

Using a hypothetical-deductive process, using a qualitative strategy and a "case study" model, we started by the identification of the differences and similarities of cyberspace in comparison to the other operational domains, a characterization of the positioning of NATO and the EU in the recognition of the cyberspace as an operational domain, and finally, an analysis was made of the impact of this decision on the Portuguese Armed Forces.

Through this investigation was possible to conclude that cyberspace is, in almost all aspects, different from the other operational domains, requiring a proper and differentiated strategic approach, and that a revision to the National Defence politic is necessary in order to accommodate a new organizational framework for cyberdefence capability, reorienting the focus from information security, to the mission accomplishment, as a military capability.

Keywords: *Cyberspace, Cyberdefence, Operational Domain, National Defence Politic*

Lista de abreviaturas, siglas e acrónimos

AR	Assembleia da República
CCD	Centro de Ciberdefesa
CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CNCS	Centro Nacional de Cibersegurança
CPOG	Curso de Promoção a Oficial General
CSI	Comunicações e Sistemas de Informação
DN	Defesa Nacional
EMGFA	Estado-Maior-General das Forças Armadas
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EUA	Estados Unidos da América
FFAA	Forças Armadas
GM	Guerra Mundial
Hip	Hipótese
IESM	Instituto de Estudos Superiores Militares
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LOBOFA	Lei Orgânica de Bases das Forças Armadas
MDN	Ministro da Defesa Nacional
MIFA	Missões das Forças Armadas
OE	Objetivo especifico
OG	Objetivo geral
OTAN	Organização do Tratado do Atlântico Norte
PEDN	Política Estratégia de Defesa Nacional
QC	Questão central
QD	Questão derivada
TIG	Trabalho de Investigação de Grupo
TII	Trabalho de Investigação Individual
TTP	Táticas, técnicas e procedimentos
UE	União Europeia
VoIP	*Voice Over Internet Protocol*

Introdução

Enquadramento e justificação do tema

Até ao início do Século XX as guerras e os conflitos desenvolviam-se apenas em dois domínios, o terrestre e o marítimo. Com a I Guerra Mundial (GM), assistiu-se ao advento da aviação e ao seu emprego nas ações militares, inicialmente como suporte às ações nos referidos domínios, autonomizando-se rapidamente com capacidade para desenvolver ações próprias ou combinadas, consolidando assim um terceiro domínio operacional, o aéreo. Já no pós II GM, e no decurso da apelidada Guerra Fria, surge, na sequência da exploração do espaço e da "corrida espacial", uma nova área de conflito, o espaço como o 4.º domínio operacional da guerra.

No último quarto do Século XX, com o advento das redes de comunicações globais, das quais a Internet será a de maior expansão e impacto, e a explosão tecnológica com a proliferação dos computadores e dos microprocessadores que se integram em todos os domínios da vida pública e privada, levam a um novo paradigma, assente numa sociedade global em que todos estão em ligação com todos, independentemente das distâncias.

Como todas as áreas de atividade humana, também esta nova dimensão passou a ser uma área de conflito de interesses e palco de ações hostis que se multiplicaram, principalmente a partir do início do Século XXI. Inicialmente, com uma preponderância das ações individuais (*hackers* ou piratas informáticos), rapidamente apropriadas por organizações criminosas (cibercrime), passando também para o nível da contestação política no ciberespaço (*hactivismo*), e por fim, como meio de atuação dos estados ou organizações terroristas contra outros estados ou na defesa dos seus interesses (ciberdefesa, ciberguerra, ciberterrorismo ou ciberespionagem).

Daí que, no desenvolvimento da utilização do ciberespaço pelos estados como palco de ação na defesa dos seus interesses e, consequentemente, potenciador de conflito, leva a que os mesmos, de forma explicita ou implícita, venham progressivamente a considerá-lo como um novo domínio operacional[1].

Perante esta tendência dos estados em considerarem o ciberespaço como um novo domínio operacional, a Organização do Tratado do Atlântico Norte (OTAN) não podia deixar de acompanhar a evolução e a tendência dos seus membros, bem como e dos principais atores da geopolítica internacional. É assim que, no comunicado final da Cimeira

[1] 4º ou 5º domínio em função de considerarem ou não o domínio espacial.

da OTAN em Varsóvia, que teve lugar em junho de 2016, a Aliança *"(...) recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.*". (OTAN, 2016c, pontos 70 e 71).

Portugal, como membro da OTAN, não pode deixar de tomar em consideração esta clara afirmação da Aliança, promovendo uma profunda avaliação do seu impacto na Política e Estratégia da Defesa Nacional (PEDN). É com este propósito que se elabora o presente Trabalho de Investigação de Grupo (TIG), procurando-se em primeiro lugar definir ou clarificar os conceitos envolvidos, prosseguindo-se com uma análise crítica e comparativa das posições assumidas, não só pela OTAN, mas também pela União Europeia (UE) e países de referência, bem como por alguns estados terceiros relevantes para a geopolítica global, avaliando por fim o impacto desta decisão na PEDN, bem como na estrutura e organização militar nacional.

A atualidade e a importância que o tema assume, quer no contexto nacional e internacional, quer no contexto académico em que se enquadra o Curso de Promoção a Oficial General (CPOG), fazem do presente um trabalho oportuno e necessário, esperando-se ainda que se revele útil e relevante contributo para PEDN.

Objeto de estudo e a sua delimitação

Define-se como objeto de estudo a assunção do ciberespaço como um novo domínio operacional e dos seus impactos estratégicos na PEDN.

Objetivos da investigação

O presente trabalho de investigação de grupo, possui como Objetivo Geral (OG):

[OG] Analisar a assunção do ciberespaço como novo domínio operacional e o impacto desta decisão na PEDN.

Para a consecução do OG supra estabelecido, concorrem, no âmbito do presente trabalho, os seguintes Objetivos Específicos (OE):

[OE1] Caracterizar o ciberespaço nas suas diferenças e semelhanças relativamente aos demais domínios operacionais;

[OE2] Analisar o impacto para as Forças Armadas (FFAA) decorrente de Portugal, no seio da OTAN, ter assumido o ciberespaço como domínio operacional.

Questões da investigação e hipóteses

Face ao enquadramento anterior e ao OG definido anteriormente, estabelece-se como Questão Central (QC):

[QC] De que forma é que o reconhecimento e a assunção, por parte da OTAN, do ciberespaço como um novo domínio operacional impacta na PEDN?

A partir da QC e tendo em vista o OE supra delineados, importa agora identificar as Questões Derivadas (QD) bem como as correspondentes Hipóteses (Hip), como possível resposta às mesmas:

[QD1] Em que medida o ciberespaço, como domínio operacional, assemelha-se ou diferencia-se dos demais espaços operacionais?

[Hip1] O ciberespaço possui características intrínsecas e genéticas muito diferenciadas dos demais domínios operacionais, fazendo com que a abordagem estratégica ao mesmo tenha que se reger por princípios próprios e diferenciados dos outros domínios.

[QD2] Que implicações decorrem para as FFAA do facto do ciberespaço ser considerado domínio operacional?

[Hip2] As FFAA ainda não têm capacidade de conduzir operações no ciberespaço e, como tal, de assumir o ciberespaço como domínio operacional.

Breve síntese da metodologia da investigação

Na elaboração e condução do presente TIG tomam-se como referências as Normas de Execução Permanente do Instituto de Estudos Superiores Militares (IESM) ACA 010 (IESM, 2015a) e ACA 018 (IESM, 2015b), de setembro de 2015, incluindo a referenciação bibliográfica sugerida, o sistema autor-data, adotando-se o estilo *Harvard-Anglia.*

A metodologia de investigação prosseguida toma como referência as Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (IESM, 2016).

Quanto à forma de raciocínio, adota-se o processo hipotético-dedutivo, porque partindo-se de um caso particular, que é uma tomada de decisão por parte da OTAN sobre o ciberespaço, concebe-se um modelo teórico que nos leva às hipóteses, cujo processo de verificação nos encaminha ao caso particular de Portugal sobre este mesmo espaço, como espaço operacional, permitindo assim uma reformulação da teoria inicial.

No que respeita à estratégia de investigação, opta-se por uma estratégia qualitativa, na medida em que estamos perante um objeto de investigação não quantificável, sobre o qual se procura um entendimento subjetivo, baseado em perceções e opiniões sobre o objeto, tendo por base observações e uma análise documental, não se tendo optado por fazer entrevistas devido à limitação de tempo.

Finalmente, como desenho de pesquisa, opta-se por um modelo de estudo de caso, em que o caso concreto é a realidade nacional, sendo o percurso da investigação estruturado em três fases, a exploratória, a analítica e a conclusiva.

Na primeira fase, exploratória, foi realizado uma pesquisa sobre o tema, estabelecida a metodologia, definida a QC e determinada a sua delimitação. O estudo foi organizado em hipóteses que servirão de linhas de condução do trabalho. Na segunda fase, durante a fase analítica, os dados referentes à pesquisa foram recolhidos, analisados e apresentados seguindo uma estratégia qualitativa. Finalmente, na terceira fase, conclusiva, serão apresentadas as respostas às QD confirmando ou não, as hipóteses, destacando os contributos da investigação e as decorrentes recomendações.

Organização do estudo

O trabalho compõe-se de quatro partes: a introdução, dois capítulos e as conclusões.

Na introdução será apresentado o objeto do estudo, o OC e os OE, num total de dois, a QC as QD e as respetivas Hip, também num total de dois, uma breve síntese metodológica finalizando-se com a presente organização do estudo.

No primeiro capítulo, através de uma breve revisão da literatura, procura-se definir o conceito geral de ciberespaço face aos restantes espaços, descrevendo as suas propriedades e a forma como o mesmo se diferencia e articula com os restantes espaços, terminando-se uma breve síntese conclusiva na qual validar-se-á ou não a Hip1.

No terceiro capítulo, pretende-se complementar a caracterização do ciberespaço já com as componentes e na perspetiva militar, caraterizando-o como domínio de operações e por fim deduzir as implicações que decorrem para as FFAA, avaliando da sua capacidade para executarem operações neste novo domínio.

Na conclusão do trabalho, apresenta-se um resumo dos resultados obtidos, procedendo-se à elaboração da resposta à QC, terminando com a apresentação de contributos e as decorrentes recomendações.

1. Ciberespaço: conceito, propriedades e articulação

"*Pois então dêem a César o que é de César e a Deus o que é Deus*"
(Biblia, 2009, p. Mateus 22:21)

1.1. No princípio era a "cibernética"

A expressão "cibernética" com origem no antigo grego, "Κυβερνήτης" (kubernétikê), com o significado de "arte de pilotar, arte de governar" (Rocha, 2003), e utilizada por Homero na Odisseia com o sentido de timoneiro, está desde a sua origem sempre associada à relação do homem com a máquina e do governo desta pelo homem.

Já no Século XX, e em plena II GM, o matemático norte-americano Norbert Wiener (1894-1964), desenvolve um conjunto de estudos e teorias em torno da "comunicação e controlo" entre humanos e sistemas, dando origem à palavra inglesa *cybernetics*, da qual derivam expressões em várias línguas com idêntico significado, traduzindo-se para o português como "cibernética". Desde então a palavra foi usada em diversas áreas do conhecimento humano, tais como as ciências sociais e económicas, até que, já nos anos 70, Alan Turing, John von Neumann e Claude Shannon, desenvolveram as teorias da informação e da computação, referindo-se à relação dos humanos com os sistemas de informação como sendo uma relação de controlo e governo cibernético. (Beer, 2001)

A explosão dos sistemas de computação e a revolução registada nas tecnologias de informação e comunicação nas últimas décadas do século XX, promoveram a utilização generalizada da expressão cibernética, da qual se extrai a prefixo *ciber* (no inglês *cyber*) como classificador de conceitos, expressões e objetos relacionados com os sistemas de informação, numa primeira fase, e com comunicações e redes de dados numa fase posterior. Já no início do século XXI, obtemos um novo vocabulário e nomenclatura que define uma nova dimensão da atividade humana que possui em comum o prefixo ciber[2].

Deste novo vocabulário e da nova dimensão da atividade humana resulta uma nova dimensão com características próprias e especificas em função da natureza da atividade, dos bens, da geografia e da sociologia que lhe estão associadas, dando origem a um novo espaço, o qual não poderia ter outra designação que não fosse ciberespaço.

[2] Fazendo-se uma pesquisa no portal da *Internet* do *Cambridge Dictionary* (2017), pelas palavras ou expressões iniciadas ou que contenham o termo *cyber*, encontram-se mais de 1000 entradas, sendo uma das famílias de palavras que apresenta um maior crescimento, com quase uma centena de novas palavras ou expressões por ano. Elas representam objetos, ações, qualificativos, conceitos, locais, etc...

1.2. **O conceito de ciberespaço**

Seria natural procurar uma definição do conceito de ciberespaço nas grandes fontes de referência e de definição de conceitos, sejam elas, as de natureza linguística, académicas ou ainda nos documentos oficiais, bem como seria expectável que este assunto se esgotasse no máximo em uma página, com a apresentação de um conceito único, inclusivo de todas as vertentes e universalmente aceite por todas as partes. Infelizmente, talvez devido à ainda reduzida maturidade, o panorama na definição do conceito de ciberespaço não é de forma alguma simples nem direto, registando-se uma grande diversidade de conceitos, o que revela por si só a transcendência deste novo espaço, o qual, possuindo características próprias, tal como veremos mais à frente, o distingue dos demais pela sua natureza imaterial, volátil, subjetiva e humana.

Tendo como referência um estudo comparativo efetuado por um especialista em segurança, da CISCO, Damir Rajnovic (2012), adaptou-se a Tabela 1, que se apresenta de seguida, na qual são identificados os vários aspetos que caracterizam o ciberespaço, em três grupos, os tangíveis, os intangíveis e os relativos a redes. Procurou-se ainda atualizar a análise para os conceitos mais recentes, nos casos em que os mesmos tenham sido atualizados desde 2012, tendo-se ainda acrescentado a análise referente ao conceito entretanto definido pela OTAN.

Tabela 1 – Comparação de conceitos de ciberespaço

	Tangíveis		**Intangíveis**					**Redes**			
	Computadores	**Hardware**	**Informação**	**Atividades**	**Aplicações e Serviços**	**Interação Humana**	**Virtual**	**Internet**	**Redes**	**Interligação**	**Comunicação**
Oxford Dictionary							V	V			V
Alemanha	V	•	V				V	V	V	V	
Austrália	V	•	•								
Canadá	V	•	V		V	V	V		V	V	
EUA	V	V	V	V		V	V	V	V	V	V
Holanda	V	•	•								
Nova Zelândia	V	V	•						V	V	V
Reino Unido			V	V	V	V	•	V	V		V
União Europeia		V	V				V				
OTAN (*Tallin Manual*)	V	•	V		V		V		V		V
ISO		V	V	V	V	V	V	V	V	V	
ITU		V	V		V	V	V	V	V	V	

Legenda: "V" - O conceito faz uma referência explícita / "•" - O conceito faz uma referência implícita.

Fonte: Adaptado de (Rajnovic, 2012)

Da análise à tabela anteriormente apresentada podem-se retirar as seguintes conclusões:

- Todas as definições reconhecem que o ciberespaço inclui elementos tangíveis;
- Todas as definições reconhecem, de forma explícita ou implícita, que a informação é uma componente do ciberespaço;
- Todos reconhecem que para além dos elementos tangíveis, o ciberespaço é constituído essencialmente por elementos intangíveis;
- Só algumas das definições é que reconhecem as atividades e as interações com o ciberespaço como fazendo parte deste;
- Na área das redes, existem definições que se centram na Internet, ignorando ou desvalorizando outras redes, havendo outras que fazem uma abordagem mais ampla às redes e às interligações como um todo, incluindo neste conjunto a Internet;
- Poucas definições são suficientemente amplas para incluírem as comunicações que não são puramente de dados, como seja a voz ou a imagem.

Infelizmente, ainda não se dispõe de uma definição oficial do conceito de ciberespaço em Portugal, nem sequer consta tal definição na Estratégia Nacional de Segurança do Ciberespaço (ENSC) (Governo, 2015a), sendo esta uma lacuna já identificada por diversas entidades, entre as quais o Centro Nacional de Cibersegurança (CNCS) e o Centro de Ciberdefesa (CCD).

Segundo o Contra-almirante Gameiro Marques (2017), está em elaboração um glossário oficial sobre um conjunto de conceitos relacionados a área ciber em Portugal, coordenado pelo CNCS e com a participação das restantes entidades com responsabilidades no ciberespaço nacional. Acrescentou ainda que o CNCS considera a definição de ciberespaço pela *International Telecommunications Union* (ITU) como sendo uma das mais completas e que provavelmente servirá de referência para Portugal (Apêndice A).

1.3. **As propriedades do ciberespaço**

Perante as dificuldades em se encontrar uma definição clara e transversalmente aceite para ciberespaço, importa então procurar caracterizá-lo e principalmente diferenciá-lo relativamente aos demais espaços. A grande maioria das representações gráficas do ciberespaço, relativamente aos demais espaços, utiliza umas das duas imagens que apresentam na figura 1.

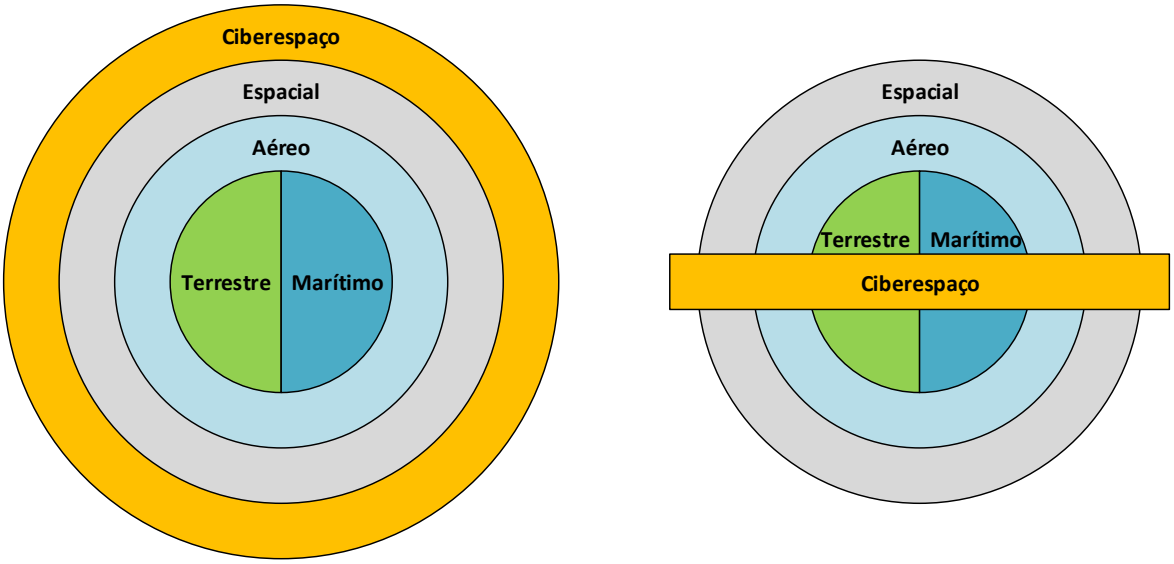

Figura 1 – Representações usuais dos cinco espaços/domínios

Fonte: Autores (2017)

Considera-se que em ambas representações o ciberespaço é representado segundo as mesmas dimensões dos restantes espaços, o que não realça nem permite realçar algumas das mais importantes características deste espaço que o diferenciam dos restantes.

Posto isto e para o efeito que se pretende obter com esta breve análise, adota-se uma outra representação do ciberespaço tomando-se como principal fonte, devidamente adaptada, uma comunicação apresentada na *5th International Conference on Cyber Conflict* (Conti, Nelson e Raymond, 2013), a partir da qual se elabora as figuras 1 e 2 e a consequente análise que se segue.

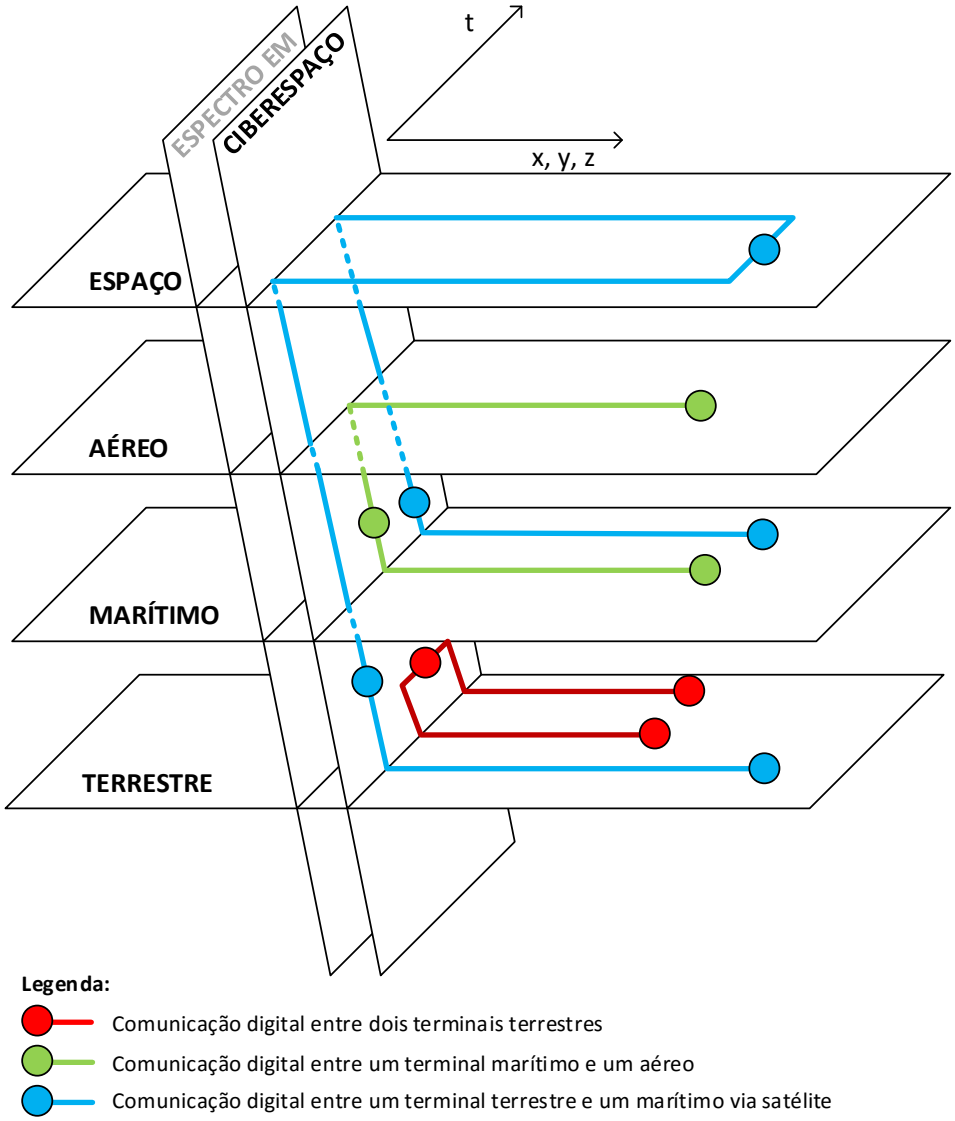

Figura 2 – Representação do ciberespaço em relação aos demais espaços

Fonte: Autores, 2017

Na figura 2 apresenta-se os quatro espaços físicos - o terrestre, o marítimo, o aéreo e o espacial - como planos horizontais.

Em planos quase perpendiculares aos quatro primeiros, representa-se o ciberespaço e, num plano secundário, um plano correspondente ao espectro eletromagnético, o qual não se constituindo como um espaço autónomo, não deixa de partilhar muitas semelhanças com o ciberespaço, estabelecendo inclusive uma relação muito intrínseca com este, mas não se confundido.

Importa ainda representar, sobre esta mesma figura e de alguma forma, a projeção das dimensões que caracterizam os espaços, enquanto conceitos quadrimensionais. Para o efeito, ter-se-á que recorrer a um artifício, que será o de se fundir num único eixo as três

dimensões físicas (largura 'x', altura 'y' e profundidade 'z') mantendo-se a representação da dimensão tempo isolada num eixo à parte. No topo da figura apresenta-se um sistema de dois eixos cartesianos que reflete este propósito, sendo que, no eixo com o sentido da largura, se representa de forma fundidas as três dimensões físicas e no eixo com o sentido da profundidade, a dimensão do tempo.

Representa-se ainda nesta mesma figura três exemplos de comunicação digital/eletrónica/eletromagnética, com o objetivo de se demonstrar como é que a informação e os processos utilizam o ciberespaço como espaço intercomunicante entre os diferentes espaços.

Importa agora observar em maior detalhe a constituição do ciberespaço. Esta varia consoante a perspetiva em que a mesma é constituída, pelo que, na figura 3, opta-se por apresentar essa constituição segundo a perspetiva das redes e segundo a perspetiva da informação, sendo que nas duas perspetivas ambas possuem três níveis denominados camadas e dimensões respetivamente.

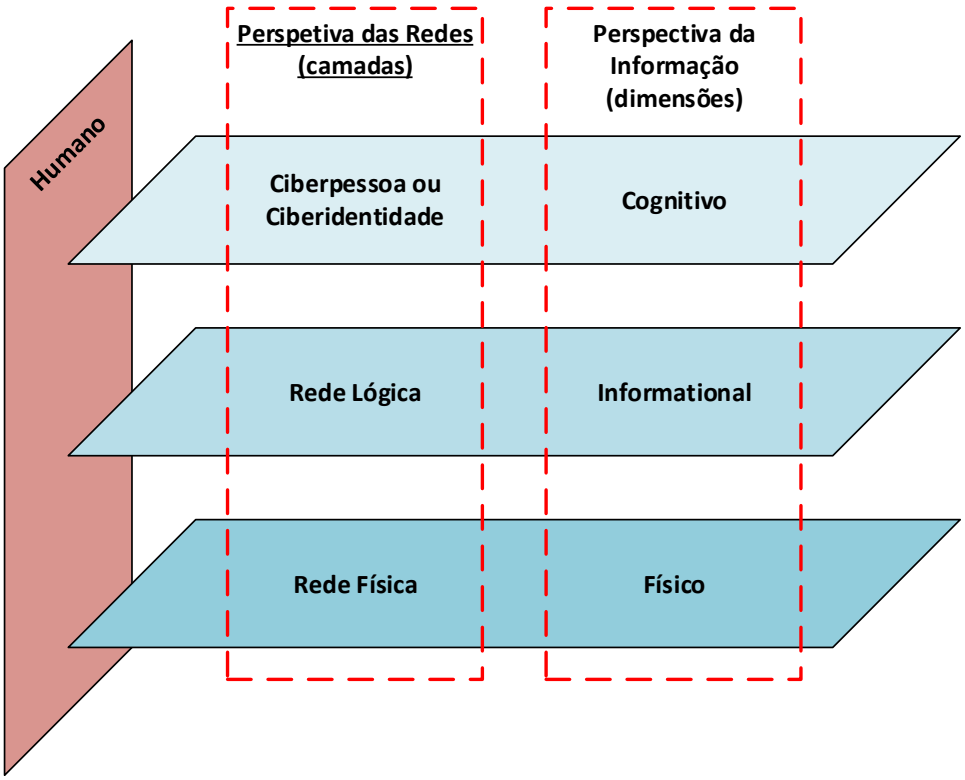

Figura 3 – Camadas componentes do ciberespaço

Fonte: Autores, 2017

Desta figura sobressaem o que já se tinha referido na secção anterior quando se analisou as definições de ciberespaço, ou seja:

- Existe uma componente tangível que se projeta na camada/dimensão física;
- A grande parte do ciberespaço é constituída por componentes intangíveis, tais como, a informação, os processos, as ciberidentidades, as relações entes elas e os aspetos sociais, elementos que se projetam nas duas camadas/dimensões superiores.

A relação do fator humano com o ciberespaço, como parte constituinte ou como mero utilizador/explorador, é sempre geradora de muita discussão sendo que, exceto no contexto militar ou em casos muito específicos, este fator não se constitui como mais uma camada ou dimensão, mas antes como um fator de sustentação e de interação de e com o ciberespaço. Com base nestas duas últimas figuras e nos considerandos que sobre as mesmas foram apresentados, enumeram-se de seguida as principais características do ciberespaço, entre as muitas que são referenciadas em múltiplos estudos, por confrontação aos restantes espaços:

- As dimensões físicas no ciberespaço quase que se anulam (apenas subsistem na medida do necessário para sustentar as componentes físicas), o que faz com que no ciberespaço desapareçam as distâncias, considerando-se que todos os elementos deste espaço estão equidistantes entre si. Daqui resulta um ciberespaço de dimensão global (1-Globalidade);
- A dimensão tempo manifesta-se de forma semelhante à dos dos restantes espaços, contudo, sem a barreira das dimensões físicas, os seus efeitos fazem-se sentir de uma forma muito mais rápida, sendo apenas limitada pela velocidade da ação ou reação humana para os despoletar ou parar (2-Imediatismo);
- O ciberespaço é transversal aos restantes espaços cruzando-os de forma quase ortogonal, mas servindo como meio de interligação imaterial ou informacional entre eles (3-Transversalidade);
- O ciberespaço possui uma capacidade de auto-replicar-se, que advém da inexistência das dimensões físicas e da sua natureza imaterial ou intangível[3] (4-Autorreplicação e proliferação);

3 Por analogia, é impossível duas pessoas ou dois objetos ocuparem um mesmo espaço físico, ou uma pessoa ou um objeto replicar-se estando presente simultaneamente em mais do que um lugar A possibilidade de poder estar simultaneamente em mais do que um lugar, é o que se denomina por ubiquidade, propriedade esta que está reservada, no nosso mundo físico-teológico, aos deuses.

- Através da ciberidentidade, no ciberespaço é possível uma pessoa ou um artefacto assuma simultaneamente diferentes identidades em diferentes contextos, permitindo ainda por esta via uma anonimização entre a identidade física e a ciberidentidade [4] (5-Anonimato e ubiquidade);
- A quase total imaterialidade dos bens e das entidades, fazem com que a presença efetiva no ciberespaço seja pouco onerosa, nivelando ou esbatendo as diferenças de capacidades entre os diferentes atores [5] (6-Desonerosidade);
- Depende do espectro eletromagnético para a sua existência a todos os níveis, ações e interações [6] (7-Espaço eletromagnético);
- É uma criação da humanidade para a humanidade, sendo um espaço que não sobreviverá a uma eventual extinção humana. Esta propriedade é a que justifica a citação do Novo Testamento da Bíblia no início do presente capítulo, permitindo elaborar o seguinte aforismo, "em o ciberespaço é de César e os demais espaços são de Deus" (8-Origem humana).

1.4. **Síntese conclusiva**

Conclui-se assim que o ciberespaço como espaço criado pela humanidade, para acomodar toda uma nova atividade nascida a partir do último quarto do Século XX, e que se caracteriza e constitui como o mundo "ciber", é na grande maioria das suas propriedades diferente dos restantes espaços, exigindo assim uma abordagem estratégica, para a sua exploração e governabilidade, regida por princípios próprios e diferenciados dos restantes domínios ou espaços.

Considera-se assim que a Hipótese 1 é válida, respondendo desta forma à Questão Derivada 1.

4 Esta anonimização do individuo ou da identidade física que corresponde a uma determinada identidade digital é o que se constitui como uma das maiores dificuldades no âmbito da cibersegurança, do cibercrime, da ciberespionagem e, obviamente, da ciberdefesa, para no apuramento de responsabilidades ou na identificação unívoca do agressor ou transgressor.

5 É possível a um único indivíduo ou a um pequeno grupo de indivíduos, com recursos limitados, provocar danos num sistema ou infraestrutura, equivalente à maioria dos países com alguma capacidade ofensivas no ciberespaço e muito superior à capacidade da generalidade dos países menos desenvolvidos. É igualmente possível a uma pequena empresa desenvolver atividades comerciais no ciberespaço que podem ombrear com grandes multinacionais, desde que disponham de um conhecimento mais próximo dos seus públicos-alvo.

6 O ciberespaço sendo um espaço assente nas telecomunicações e na eletrónica utiliza os princípios que regem o espectro eletromagnético na sua máxima extensão, desde as comunicações wireless, até ao armazenamento de dados que são frequentemente efetuados sobre a forma de magnética. No entanto, o espectro eletromagnético possui uma existência própria independente do ciberespaço, existindo tal como os espaços físicos muito antes do ciberespaço.

2. O ciberespaço como domínio operacional

> "*(…) não há coisa mais difícil de tratar, de êxito mais duvidoso nem de manejo mais perigoso do que aventurar-se alguém a impor novas instituições, (…)*"
>
> (Maquiavel, 1976, p. 35)

2.1. Enquadramento

Em intervenção na Assembleia da República (AR)[7] subjacente à cimeira da OTAN em Varsóvia, o Ministro da Defesa Nacional afirmou que "na área da ciberdefesa se esperam resultados promissores da Cimeira: a consolidação definitiva do ciberespaço como um *domínio operacional*, como um verdadeiro e novo teatro de operações – para além da terra, do mar e do ar" (Lopes, 2016, p. 9). Esta declaração, consentânea com as resoluções tomadas pelos países da OTAN em Varsóvia e que, entre outras, reconhece o ciberespaço como domínio das operações, exige à Aliança a capacidade de se proteger e conduzir ciberoperações, similarmente ao que vem fazendo nos demais domínios (OTAN, 2016c).

Neste capítulo pretende-se, à luz das referências doutrinárias usuais, analisar e caraterizar o ciberespaço enquanto dimensão operacional e abordar as implicações que daí decorrem para as FFAA, nomeadamente a adequação da estrutura de ciberdefesa às missões e desafios resultantes deste novo domínio de operações.

2.2. Caraterização ciberespaço na perspetiva operacional e militar

É hoje comummente aceite que, no atual ambiente complexo onde a ameaça está permanentemente em evolução, a OTAN e os países que a integram enfrentam adversários que utilizam o ciberespaço como uma nova dimensão para desenvolver atividades ilícitas de natureza diversa, tirando partido das múltiplas oportunidades que o ciberespaço permite, no sentido de ganhar vantagem ou, de algum modo, perturbar ou interromper operações em curso e degradar a confiança dos países nos sistemas e tecnologias de informação e comunicações de que são proprietários. Consequentemente, a Aliança (2014a) definiu que a proteção das suas redes e sistemas, através da implementação de um programa robusto de ciberdefesa, constitui um elemento crítico para o bom cumprimento da sua missão, impondo-se desde logo uma perceção similar do ciberespaço enquanto novo domínio de operações (OTAN, 2016b, p. 1), condição determinante ao desenvolvimento harmonioso das capacidades nacionais.

[7] Em 23 de junho de 2016.

A avaliação do impacto do ciberespaço como domínio operacional exige primariamente o entendimento dos conceitos subjacentes principais[8], por via da doutrina nacional, da Aliança ou de países de referência, nomeadamente os que se referem a:

- Ambiente operacional: "o conjunto de condições, circunstâncias e fatores influenciadores que afetam o emprego de forças militares e influenciam as decisões do comandante" (Exército, 2012, p. 17).
- Ciberespaço: domínio global e virtual criado pela interligação de todas as redes de comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas (OTAN, 2016b, p. 2).
- Ciberdefesa: meios para alcançar e executar medidas defensivas para reagir contra ciberataques e mitigar os seus efeitos, preservando e restaurando a segurança das comunicações, da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas (OTAN, 2014b).

A OTAN (2016a, p. 5) define domínio como a esfera de interesse e influência em que as atividades, funções e operações são realizadas de modo a cumprir missões e exercer o controlo sobre um adversário, a fim de se obterem os desejados resultados. A doutrina de referência dos Estados Unidos da América (EUA) (US JCS, 2013) e da OTAN (2016a, p. 2) e a análise bibliográfica efetuada, permitem identificar mais algumas características do ciberespaço, para além das já identificadas no capítulo um (de âmbito genérico), em especial aquelas que são de aplicação específica ao ciberespaço enquanto domínio operacional e militar, nomeadamente:

- Possibilita a ação remota que é de difícil identificação quanto à origem (9-Ação remota), caraterística derivada por conjugação das (1-Globalidade), (2-Imediatismo) e (5-Anonimato e ubiquidade);
- Exige poucos recursos de acesso propiciando o confronto assimétrico (10-Conflito assimétrico) característica derivada do (5-Anonimato e ubiquidade) e (6-Desonerosidade);
- Permite a interação ou, melhor, a presença, de amigos e adversários em infraestruturas de diferente natureza - civis ou militares, públicas ou privadas, nacionais ou internacionais,

[8] Sem prejuízo de outros conceitos abordados no Apêndice A.

coexistindo as mais diferenciadas capacidades (11-Coexistência distribuída) resultante da conjugação das características da (1-Globalidade), (2-Imediatismo), (4-Autorreplicação e proliferação) e de (5-Anonimato e ubiquidade).

Caraterizado o ciberespaço como uma dimensão diferenciada, importa avaliar se este pode ser, ou não, qualificado como domínio da guerra. Para o efeito, recorremos a uma métrica padrão (OTAN, 2016a cit. por Camelo, 2017, p.17) que determina a verificação dos seguintes pressupostos:

- A existência de capacidades específicas para operar nesse domínio, o que se verifica por via da necessidade de formação, competência e treino específicos, para além de táticas, técnicas e procedimentos (TTP) e sistemas operacionais completamente distintos dos restantes domínios.
- O ciberespaço como dimensão de operações não estar totalmente englobado por um outro domínio, o que se verifica até porque o ciberespaço é o elo comum aos restantes domínios.
- A existência da presença partilhada de capacidades amigas e oponentes, condição em que o ciberespaço é referência, pela facilidade e baixo custo de acesso, proporcionando conflitos assimétricos.
- Permitir exercer o controlo sobre eventuais oponentes através da influência ou dominância, requisito também verificado pelo controlo parcial e localizado no tempo de determinada parte do ciberespaço, pela negação de acesso ao oponente, ou, ainda, em apoio das Operações de Informação.
- Capacidade de estabelecer sinergias com os outros domínios, condição em que o ciberespaço é referência pela possibilidade de apoiar ações desenvolvidas nos restantes domínios, requerendo a integração no planeamento das operações.
- Permitir desenvolver ações assimétricas através dos outros domínios, nomeadamente pelo facto de muitas das ações no ciberespaço exigirem reduzidos investimentos quando comparados com ações nos outros domínios, em contraponto aos efeitos maximalistas que podem ser produzidos nos adversários.

Assente no crescimento exponencial das tecnologias disponíveis no mercado, os agentes promotores de atividades maliciosas vêm incrementando, com uma frequência absolutamente inacreditável, as TTP associadas ao ciberespaço, tornando cada vez mais difícil a proteção. Conforme sublinhado por um antigo assistente do diretor do *Federal*

Bureau of Investigation para a cibersegurança (Shaw cit. por Ackerman, 2015a), pese embora a ideia geral subjacente à segurança do ciberespaço assentar na cooperação e partilha, importa explicitar o seu real significado sob pena de poder determinar, por excesso de informação, a paralisia operacional. "De facto nesta era, já não da *Internet of Things* mas da *Internet of Everything*, a preservação do ciberespaço de interesse nacional, numa perspetiva securitária, está desde logo alicerçada em mecanismos e processos de cooperação e partilha de *cyber intelligence*, nomeadamente a informação associada a ameaças identificadas e a vulnerabilidades detetadas, ou exploradas por ações hostis, por forma a que, com oportunidade, seja extraído conhecimento acionável" (Camelo, 2016).

2.3. **Operacionalização do ciberespaço**

Assumido o ciberespaço como domínio da guerra ressalta a necessidade de se proceder à respetiva conceptualização operacional, ou seja: analisar como se organiza o ciberespaço do ponto de vista das operações militares e como estas se categorizam neste ambiente, de modo a poderem ser alcançados objetivos no e através do ciberespaço.

2.3.1. OTAN

Posteriormente a alguns dos estados membros, também a Aliança assumiu o ciberespaço como domínio operacional (2016c), tendo procedido à sua operacionalização (OTAN, 2017), estruturando-o numa lógica de seis camadas conforme apresentado na Figura 4.

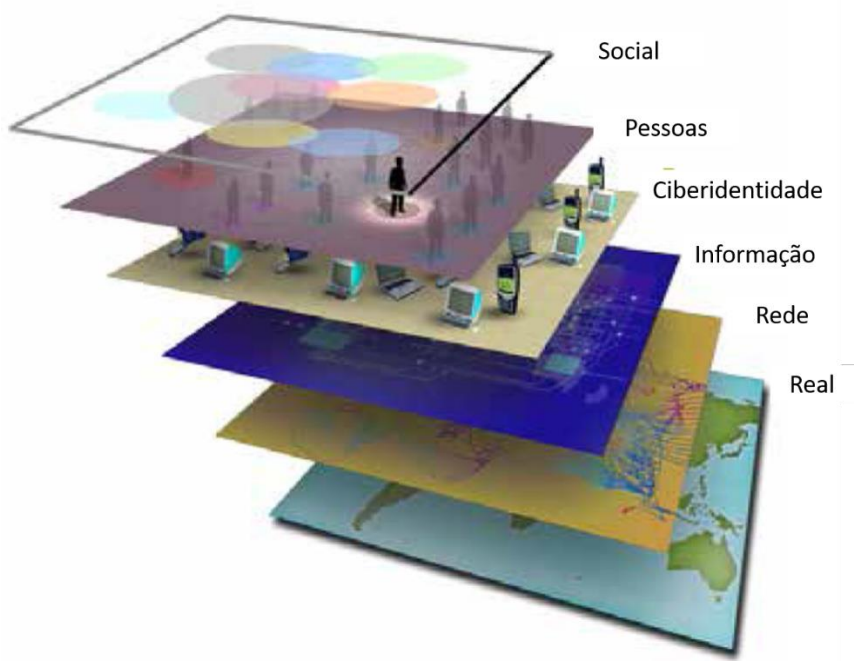

Figura 4 – Estrutura do ciberespaço

Fonte: Adaptado de (OTAN, 2017, p. 18)

Conforme a doutrina apresentada recentemente pela OTAN (2017, p. 33), as operações no ciberespaço categorizam-se:

- Quanto à tipologia:
  - Operações Defensivas: que visam preservar a capacidade de usar o ciberespaço e que englobam operações ativas e operações passivas;
  - Operações Ofensivas: que visam projetar força para atingir objetivos no e através do ciberespaço, englobando as operações de apoio e as operações ofensivas.
- Quanto aos efeitos:
  - Negar;
  - Degradar;
  - Interromper;
  - Destruir.
- Em função de apoio:
  - Manobra;
  - Fogo;
  - Comando e controlo;
  - Informações;
  - Informação;
  - Sustentabilidade;
  - Proteção da força;
  - Cooperação civil militar.
- Quanto à gestão do risco[9]:
  - Aceitar;
  - Evitar;
  - Transferir;
  - Mitigar.

[9] Pode incluir uma ou uma combinação das ações elencadas.

2.3.2. UE

A UE considera que o ciberespaço é um domínio onde os adversários procuram obter vantagens assimétricas através de ações encobertas sob a capa do anonimato (numa lógica de não atribuição), de modo a obterem objetivos militares e, ultimamente, sobretudo com objetivos políticos. Resulta assim o ciberespaço ser entendido como um domínio igualmente crítico para o cumprimento das suas missões e sobrevivência dos estados membros, devendo ser considerado como domínio operacional (UE, 2016, p. 10).

No seu conceito de ciberdefesa para apoio às operações (2016, p. 32), a UE define que as ciberoperações têm como finalidade garantir a liberdade de ação no ciberespaço de forma a que sejam alcançados os objetivos operacionais, negar a liberdade de ação aos adversários e potenciar outras atividades operacionais. Para tal articulam-se em:

- Operações em redes federadas de missão;
- Operações defensivas;
- Operações ofensivas.

2.3.3. Impacto na doutrina militar

Fruto deste novo domínio das operações, as FFAA dos EUA têm feito progressos consideráveis relativamente às TTP no ciberespaço, nomeadamente pela capacidade de integrar ciberataques com os métodos tradicionais de guerra eletrónica disponibilizando uma capacidade sofisticada aos comandantes operacionais em todas as fases da guerra de modo a potenciar os efeitos eletromagnéticos e ciberespaço, ou, em alternativa, empregar essa capacidade como um multiplicador de força (Taylor, 2016, pp. 36-37).

Resulta pois que a conceptualização operacional do ciberespaço, determina que as FFAA estejam estruturadas, nas várias dimensões da sua capacidade de ciberdefesa, para acompanharem a mudança de paradigma, de uma filosofia assente na necessidade de proteção do ciberespaço de interesse nacional, visando a segurança, disponibilidade e integridade das comunicações e sistemas de informação (CSI), para uma nova dimensão em que as capacidades cibernéticas, *per se* ou integradas com as demais, concorrem para a obtenção de objetivos no e através do ciberespaço.

2.4. **Ciberdefesa em Portugal**

2.4.1. Quadro normativo

Mercê das ameaças e riscos que o ciberespaço pode apresentar, por oposição às imensas oportunidades que representa para todas as facetas da sociedade contemporânea,

também em Portugal a questão do ciberespaço vem determinando uma abordagem político-estratégica, mormente pelo estabelecimento de um quadro normativo e conceptual a montante. Desde logo, esta temática foi abordada como questão essencial no Conceito Estratégico de Defesa Nacional (CEDN), que sublinha o caráter dual do ciberespaço, enquanto promotor da globalização e da revolução tecnológica mas, simultaneamente, proporcionando um novo vetor de propagação de ameaças e riscos que exige uma resposta capaz dos estados, considerando que "os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna" (Governo, 2013, p. 16). Entre outros, o CEDN (Governo, 2013, p. 34) define, como linha de ação prioritária no domínio da cibercriminalidade, o levantamento da capacidade de ciberdefesa considerando que "As alterações estruturais no ambiente de segurança e a natureza das ameaças à segurança nacional implicam uma capacidade de resposta diferente das Forças Armadas" (Governo, 2013, p. 36).

Consequentemente, esta temática foi incorporada no Conceito Estratégico Militar, materializando-se nos cenários gerais de emprego das FFAA, mais especificamente no cenário relativo à segurança e defesa do território nacional (TN) e dos cidadãos, que estabelece o subcenário da Ciberdefesa. Este subcenário diz respeito à intervenção das FFAA no âmbito da ciberdefesa, através da aplicação de medidas de segurança que garantam a salvaguarda da informação e a proteção das infraestruturas de CSI das FFAA contra ciberataques, bem como, o apoio, no caso de um ciberataque, na proteção e defesa das infraestruturas críticas nacionais e do governo eletrónico do Estado (CCEM, 2014).

As Missões das FFAA (MIFA), no âmbito de segurança e defesa do TN e dos cidadãos, especificam[10] que a ciberdefesa englobando a aplicação das medidas de carácter defensivo e se necessário ofensivo contra ataques cibernéticos, a fim de garantir a salvaguarda da informação e a proteção das infraestruturas de CSI das FFAA, bem como, o apoio na proteção e defesa das infraestruturas criticas nacionais e do governo eletrónico do Estado (MDN, 2014a, p. 3).

Em 2013 foi difundida a Orientação Política para a Ciberdefesa, visando preparar as FFAA para o "ambiente do moderno campo de batalha, cada mais descontínuo e multidimensional, constatando -se que as operações militares têm vindo progressivamente a incluir o desenvolvimento de operações em redes de computadores (defensivas, de

[10] M1.6.

exploração e ofensivas), juntando aos tradicionais espaços de atuação (terra, mar e ar) também o ciberespaço" (MDN, 2013, p. 31977). Para o efeito, elenca os seguintes aspetos principais:

- As atividades de ciberdefesa são orientadas para atender às necessidades da defesa nacional visando assegurar a utilização do espaço cibernético, impedindo ou dificultando o seu uso contra os interesses nacionais nos tradicionais espaços de atuação (terra, mar e ar) e também no ciberespaço (MDN, 2013, p. 31978).
- As FFAA dependem, cada vez mais, da livre utilização do ambiente de informação e do próprio ciberespaço para conduzirem todo o espectro de operações.

A temática central do presente capítulo é claramente abordada neste documento de nível politico-estratégico, afirmando que "o ciberespaço constitui um novo domínio operacional, onde podem vir a ser conduzidas operações militares e onde o levantamento de mecanismos de proteção e defesa obedece à mesma lógica e fundamentos que caraterizam a Segurança e a Defesa do Estado. Com efeito, as missões das FFAA dependem, cada vez mais, da livre utilização do ambiente de informação e do próprio Ciberespaço para conduzirem todo o espectro de operações" (MDN, 2013). Preconiza ainda a necessidade de estabelecer uma estrutura de comando e controlo da ciberdefesa nacional, a incluir no processo de revisão da Lei Orgânica de Bases das FFAA (LOBOFA) e da lei orgânica do Estado-Maior-General das Forças Armadas (EMGFA), contemplando a existência de um órgão com caráter de orientação estratégica-militar das atividades de ciberdefesa e uma capacidade militar de resposta operacional a ciberataques e a incidentes informáticos. Para o efeito preconiza a constituição do CCD, na dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), como órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas (MDN, 2013, p. 31978).

Posteriormente e no seguimento da Lei Orgânica do EMGFA (Governo, 2014), foram especificadas as atribuições do CCD, merecendo especial destaque, por estar intrinsecamente ligada ao objeto deste capítulo e ao tema do trabalho, a incumbência de "ao CCD compete assumir a direção e coordenação da capacidade nacional de ciberdefesa, nomeadamente conduzir operações militares no ciberespaço" (Governo, 2015b, p. 5287).

Por último e em 2015, foi publicada a ENSC, com o objetivo de "aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das

infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas" (Governo, 2015a, p. 3738). Este documento fixa seis eixos de intervenção sendo que, no âmbito da estrutura de segurança do ciberespaço (Eixo 1), especifica a necessidade de "implementar, desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional" (Governo, 2015a, p. 3740).

2.4.2. Estrutura orgânica

O Plano para a Edificação da Capacidade de Ciberdefesa é o documento enformador da estrutura da ciberdefesa (EMGFA, 2013, pp. 12-13), fixando nomeadamente:

- As sua capacidades:
  - Deteção e resposta a ciberincidentes;
  - Monitorização permanente das redes;
  - Ferramentas de *intelligence situational awareness*;
  - Módulos/equipas de ciberdefesa;
  - Necessidade de mecanismos de garantia da continuidade de serviços;
  - Análise forense;
  - Mecanismos de coordenação nacional e internacional.
- A sua estrutura:
  - Centro de Ciberdefesa;
  - Quatro *Computer Incident Response Capability*[11] com a missão de protegerem a integridade, confidencialidade e disponibilidades das CSI á sua responsabilidade.

Da análise à estrutura de ciberdefesa, nos seus órgãos constituintes, constata-se que estes, por via do estipulado no plano de edificação, têm apenas especificado o seu efetivo em pessoal, não estando abordados com a profundidade necessária os aspetos relativos à articulação funcional (ou departamental) de cada um dos órgãos. No que respeita ao CCD,

[11] EMGFA, Marinha, Exército e Força Aérea.

o plano menciona a existência de duas subestruturas[12], afigurando-se necessário adequar a estrutura de topo das FFAA ao quadro de competências legais (Governo, 2015b, p. 5287). Esta disfuncionalidade, numa primeira fase situada no âmbito da organização e pessoal, tem especial impacto na impossibilidade de execução de quase todo o espetro de operações no ciberespaço. Esta perceção, da inadequação da estrutura existente, mormente pelo impacto do ciberespaço ser um domínio das operações, é partilhada nas FA dos diversos países, suscitando-se assim, no caso nacional, de fazer evoluir o CCD para uma estrutura tipo comando de componente, com dimensão adequada às necessidades nacionais e que seja capaz de lidar com o paradigma do ciberespaço ser domínio das operações militares.

O incremento do conceito tradicional de ciberdefesa por via de se considerar a utilização de capacidades cibernéticas para se alcançar objetivos no/através do ciberespaço e a integração no planeamento de operações como um fim ou elemento multiplicador do potencial de combate, requer novas e mais exigentes competências que só poderão ser alcançadas com formação muito específica e sobretudo, com uma permanência prolongada no manuseamento dos sistemas (*cyber warriors*), requisitos incompatíveis com a rotatividade e os processos de desenvolvimento das carreiras militares.

No contexto de combate às ciberameaças[13] as FFAA deverão concorrer para a prossecução da segurança do ciberespaço nacional nas duas vertentes, função do impacto e do risco social associado: no âmbito da cibersegurança setorial da Defesa Nacional através de uma colaboração ativa com as restantes órgãos, forças e serviços de segurança e no âmbito das responsabilidades intrínsecas da defesa nacional, nomeadamente da ciberdefesa, quando as ameaças, por apresentarem um maior poder disruptivo possam colocar em risco a segurança e defesa do Estado.

A avaliação das estruturas existentes terá de ser previamente antecipada pela clarificação do conceito que está no âmago do presente trabalho. Ou seja, a assunção do ciberespaço como domínio operacional traduz-se obrigatoriamente na capacidade das FFAA serem capazes de conduzir operações nesta dimensão. Por similaridade com o que acontece nos demais domínios relativamente à tipologia dos objetivos específicos das respetivas componentes, as operações no ciberespaço podem ser definidas pelo emprego de cibercapacidades para alcançar objetivos no ou através do ciberespaço.

[12] Repartição de Coordenação e Repartição de Operações em Redes de Computadores.
[13] Tradicionalmente ações de *spear phishing*, comprometimento de redes estratégicas, negação do serviço, exploração de vulnerabilidades e desinformação.

2.5. **Síntese conclusiva**

A quarta revolução industrial (Schwab, 2016), promotora da convergência das tecnologias digitais, físicas e biológicas, tem no ciberespaço o seu elemento de alavancagem, promovendo extraordinários avanços e desenvolvimentos em todos os setores de atividade. Paradoxalmente, o mesmo ciberespaço potenciou o aparecimento de novas ameaças e riscos que exigem dos estados, nomeadamente ao nível das suas FFAA, respostas compatíveis.

A assunção do ciberespaço como domínio operacional teve como principal impacto a mudança de abordagem, de uma perspetiva de ciberdefesa centrada na segurança da informação para uma perspetiva orientada para o cumprimento da missão. Consequentemente, as principais implicações decorrem da necessidade de se proceder a um reajustamento da estrutura operacional, nas várias vertentes de edificação da ciberdefesa, que habilite as FFAA a utilizarem o ciberespaço para o cumprimento das suas missões.

Dos elementos recolhidos e da análise da estrutura de ciberdefesa nacional, nomeadamente ao nível do CCD, permite concluir do desajustamento deste órgão para assumir o mencionado novo paradigma, mormente por via da inexistência de uma estrutura orgânica e funcional compatível com os requisitos operacionais, funcionais e técnicos mínimos necessários à condução de operações militares no ciberespaço. Esta vulnerabilidade só poderá ser colmatada por via da implementação de uma estrutura alicerçada numa lógica de comando de componente, que, aliás, é o que conceptualmente decorre de um domínio operacional. Para igual conclusão concorre também a inexistência de um verdadeiro plano de edificação de capacidade de ciberdefesa que permita, em todos os seus elementos constituintes, assumir o ciberespaço como nova área de operações e definir as responsabilidades dos diferentes níveis (operacional e tático) de decisão e execução. Analisadas as implicações e avaliada a estrutura e organização existentes, considera-se validade a Hip2, respondida a QD2 e, consequentemente, alcançado o OE2.

Conclusões

O presente trabalho, sobre o *ciberespaço como 5.º domínio operacional: impacto estratégico na política de Defesa Nacional*, visou avaliar e identificar os efeitos que uma decisão como a que foi tomada pela OTAN na cimeira de Varsóvia, em 2016, pode afetar a PEDN, bem como esta se poderá refletir na implementação da capacidade de ciberdefesa. Para tal, estabeleceu-se como QC: de que forma é que o reconhecimento e a assunção, por parte da OTAN, do ciberespaço como um novo domínio operacional impacta na PEDN?

O percurso da investigação, orientado no sentido de responder à QC, foi desenvolvido, baseado no método hipotético-dedutivo, compreendendo as seguintes etapas:

- Recolha de dados e pesquisa bibliográfica para a formulação da QC e circunscrever o objeto da problemática em estudo;
- Estabelecimento do modelo de análise, com base na QC, e determinação das QD e das respetivas hipóteses;
- Verificação das hipóteses, através da análise dos dados obtidos por via da documentação compilada e com recurso a um desenho de pesquisa por "estudo de caso", sendo o caso concreto a realidade portuguesa.

O produto do trabalho de investigação foi sistematizado em dois capítulos:

- Um primeiro, no qual se procurou estabelecer o conceito e as propriedades de ciberespaço por confrontação aos demais domínios: terrestre, marítimo, aéreo e espacial. A análise teve por objetivo, por um lado, ser consentânea com o Capítulo 2, mas também determinar se as premissas aplicáveis aos demais domínios são ou não também aplicáveis ao ciberespaço;
- O segundo, orientado para a problemática expressa no título do trabalho, procede à análise e caracterização do ciberespaço na perspetiva militar procurando entender a sua conceptualização operacional por força de organizações de referência, especificamente a OTAN, a UE e os EUA. Este capítulo conclui com a análise e identificação dos efeitos do ciberespaço como domínio operacional na ciberdefesa em Portugal, mormente pelo impacto que poderá gerar no estabelecimento da PEDN.

Na confrontação entre as proposições de partida e os resultados efetivamente alcançados pelo estudo aqui explicitado, permitiu concluir o seguinte:

- Hip1 – O ciberespaço, pelas suas características intrínsecas e genéticas diferencia-se claramente dos demais domínios, exigindo por isso uma

abordagem estratégica, também ela, diferenciada e com princípios próprios e inovadores.

- Hip2 – A assunção do ciberespaço como domínio operacional provoca uma mudança da perspetiva da ciberdefesa centrada na segurança da informação, para uma nova perspetiva orientada para o cumprimento da missão, requerendo assim uma reavaliação do enquadramento e articulação estrutural desta capacidade e, consequentemente, uma revisão ou reajustamentos da PEDN para melhor incorporar os reajustamentos orgânicos identificados.

Face ao que precede, é então possível formular a seguinte resposta à QC:

A assunção por parte da OTAN de considerar o ciberespaço como um novo domínio operacional, em igualdade de importância com os domínios terrestre, marítimo e aéreo, bem como o facto de Portugal ter subscrito esta alteração de conceito, impõe que a nível nacional se proceda ao consequente reajustamento da estrutura operacional, com especial enfoque para a ciberdefesa. Com efeito, exige-se desde logo uma mudança de perceção do ciberespaço passando este a ser entendido como plataforma para o desenvolvimento de operações de forma a habilitar a que Portugal, através das suas FFAA, sejam capazes de atuar dentro dos parâmetros, requisitos e procedimentos estabelecidos no seio da Aliança, assim como cumprirem os objetivos no âmbito da defesa nacional, assumindo a incontornável responsabilidade no âmbito da segurança do ciberespaço nacional.

Tendo em conta a diferenciação das características do ciberespaço relativamente aos demais espaços, e consequentemente, as diferenças na forma de atuar, é inegável que existe algum impacto na PEDN, pelo que se torna necessário proceder à revisão dos principais elementos da Política de Defesa Nacional, por forma a dotá-los com os instrumentos necessários a esta nova realidade operacional.

Como limitações ao presente TIG, considera-se que a maior limitação deriva precisamente das características formais, quer pela sua dimensão e estrutura, quer pelo tempo em que o mesmo tem que ser elaborado. Por exemplo, teria sido interessante ter-se efetuado uma análise à forma como outros países, aliados ou não, têm vindo promover as devidas adaptações para acolherem o ciberespaço como novo domínio operacional, identificando as soluções preconizadas e os efeitos alcançados. No entanto e realisticamente, essa análise, por mais breve que fosse, estenderia a dimensão deste trabalho em moldes considerados não apropriados ao conceito vigente no curso.

Também se gostaria de se ter aprofundado as consequências que resultam das características tão próprias do ciberespaço, designadamente o esbater das fronteiras ou da delimitação entre ameaça externa e interna, e de que forma é que se poderá gerir a intervenção das FFAA face às limitações constitucionais a que estas estão sujeitas no domínio da sua atuação na segurança interna. Exemplo disso será, perante uma ação hostil contra uma infraestrutura crítica/estratégica, e sabendo-se que no âmbito das forças de segurança não está prevista a criação de qualquer capacidade similar à prevista para ciberdefesa, questiona-se qual será a margem de atuação na defesa dessa infraestrutura critica/estratégica. Por certo, estes tópicos abrem espaços de discussão para novas e futuras investigações, em diversas vertentes, entre as quais as que foram apontadas como áreas não tratadas devido às limitações do próprio formato do trabalho.

Bibliografia

Banks, S. & Stytz, M., 2014. Toward Attaining Cyber Dominance. *Strategic Studies Quarterly*, Spring, pp. 55-87.

Ackerman, R. K., 2015a. Destructive Cyber Attacks Increase in Frequency, Sophistication. *Signal*, July.

Ackerman, R. K., 2015b. Convergence Dominates Army Cyber Activities. *Signal*, October, pp. 39-41.

AFCEA, 2016a. DHS Expands Cyber Work Force. *Signal*, December.p. 9.

AFCEA, 2016b. Millennials May Present Insider Cyberthreat. *Signal*, December.p. 9.

Anon., 2017. *Cambridge Dictionary Online.* [Em linha]

Disponível em: http://dictionary.cambridge.org/

[Acedido em 21 02 2017].

AR, 2009. *Aprova a Lei Orgânica de Bases da organização das Forças Armadas (Lei Orgânica nº 1-A/2009).* Lisboa: Diário da República.

Armée de l'Air, 2015. *Réflexions sur le cyber: quels enjeux?.* s.l.:Ministére de la Defense.

Australia Government, 2016. *Australia's Cyber Security Strategy.* [Em linha] Disponível em: https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

[Acedido em 2 3 2017].

Babcock, C., 2015. Preparing for the Cyber Battleground of the Future. *Air & Space Power Journal, 29(6),* pp. 61-73..

Beer, S., 2001. *What is Cybernetics?.* [Em linha]

Disponível em: https://pdfs.semanticscholar.org/a852/6b324bc7b236c57ed0e0b65a4e6311cd1295.pdf [Acedido em 21 02 2017].

Biblia, 2009. *Biblia Sagrada, Novo Testamento.* 2.ª ed. Lisboa: Sociedade Biblica de Portugal.

Brandes, S., 2013. The Newest Warfighting Domain: Cyberspace. *Synesis: A Journal of Science, Technology, Ethics, and Policy Volume 4*, Volume 4, pp. G90-95.

Camelo, L. F., 2016. *Cyber Intelligence - CYI 6232.* Washington D.C.: National Defense University.

Camelo, L. F., 2017. *Contributos para uma estratégia nacional de ciberdefesa (TII CPOG 2016/2017).* 1º draft ed. Lisboa: IUM.

Canada Government, 2010. *Canada's Cyber Security Strategy.* [Em linha] Disponível em: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf [Acedido em 2 3 2017].

Caton, J. L., 2015. *Army Support of Military Cyberspace Operations: joint contexts and global.* s.l.:The United States Army War College.

CCEM, 2014. *Conceito Estratégico Militar.* s.l.:Conselho de Chefes de Estado-Maior.

Chezem, J., 2015. Air Force Cyber Mission Success Depends on Culture Change. *Signal,* October, pp. 42-45.

CNCS, 2017. *Portal do CNCS.* [Em linha]

Disponível em: https://www.cncs.gov.pt/recursos/glossario/ [Acedido em 1 3 2017].

Conti, G. N. J. e. R. D., 2013. *Towards a Cyber Common Operating Picture.* Tallin, NATO CCD COE.

Cutchins, C., 2015. *Engaging Millennials: The Military Way.* [Em linha] Disponível em: http://www.franklinstreet.com/engaging-millennials-the-military-way

[Acedido em 19 março 2016].

David, J., 2016. *How Do Cyber Operations Look in 2025?.* [Em linha] Disponível em: http://www.cyberdefensereview.org/ [Acedido em 21 fevereiro 2017].

EMGFA, 2013. *Plano para a edificação da capacidade de ciberdefesa nacional,* Lisboa: Estado-Maior-General das Forças Armadas.

EU, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,* Brussels: European Union.

European Parliament, 2011. *Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU,* Bruxelas: European Parliament.

Exército, 2012. *OPERAÇÕES (PDE 3-00).* s.l.:Exército.

Exército, 2014. *Tática das Operações de Combate (PDE 3-01-00) Vol. 1.* 1º Draft ed. Lisboa: Estado-Maior do Exército.

Exército, 2015. *Normas de Gestão de Projetos do Exército.* Lisboa: Divisão de Planeamento de Forças do Estado-Maior do Exército.

Franz, T., 2011. The Cyber Warfare Professional: Realizations for Developing the Next Generation. *Air & Space Power Journal: Realizations for Developing the Next Generation,* pp. 87-99.

GAO, 2004. *Combating Terrorism Evaluation of Selected Characteristics in National Strategies Related to Terrorism,* Washington, D.C. 20548: General Accounting Office.

GAO, 2011. *DoD Faces Challenges In Its Cyber Activities,* Washington, D.C. 20548: General Accounting Office.

Germany Government, 2011. *Cyber Security Strategy for Germany.* [Em linha] Disponível em: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile

[Acedido em 2 3 2017].

Governo, 2013. Conceito Estratégico de Defesa Nacional (Resolução do Conselho de Ministros n.º 19/2013). *Diário da República,* 5 abril.

Governo, 2014. Lei orgânica do EMGFA (aprovada pelo Decreto-Lei n.º 184/2014, de 29 de dezembro). *Diário da República,* 29 dezembro.

Governo, 2015a. Estratégia Nacional de Segurança do Ciberespaço (Aprovada pela Resolução do Conselho de Ministros n.º 36/2015, de 28 de maio). *Diário da República. 1ª série - N.º113,* 12 junho, pp. 3738-3742.

Governo, 2015b. Orgânica Interna do EMGFA (aprovado pelo Decreto Regulamentar nº13/2015 de 31 de julho). *Diário da República,* 31 julho, pp. 5275-5295.

IDN, 2013. *Estratégia da Informação e Segurança no Ciberespaço.* Lisboa: Instituto da Defesa Nacional.

IESM, 2015a. *NEP/ACA 10 - Trabalhos de Investigação.* 1.ª ed. Lisboa: IESM.

IESM, 2015b. *NEP/ACA 18 - Regras de Apresentação e Referenciação para os Trabalhos Escritos a Realizar no IESM.* 1.ª ed. Lisboa: IESM.

IESM, 2016. *Orientações metodológicas para a elaboração de trabalhos de investigação - Cadernos do IESM n.º 8.* 1.ª ed. Lisboa: IESM.

IISS - The International Institute for Strategic Studies, 2015. *Evolution of the Cyber Domain.* Oxon: Routledge.

ISO/IEC, 2011. *ISO/IEC 27032 Guidelines for cybersecurity ,* Genebra: ISO/IEC.

ITU, 2008. *Recommendation ITU-T X.1205 - Overview of cybersecurity.* 1.ª ed. Genebra: ITU.

Janczewski, L. J. & Colarik, A. M., 2008. *The U.S. Military Response to Cyber Warfare.* New York: s.n.

Jontz, S., 2016a. Taking Cyber War to the Front Lines. *Signal*, October, pp. 20-23.

Jontz, S., 2016b. Wining Wars at the Speed of Cyber, Not Acquisition Cycles. *Signal*, December, p. 40.

Kreisher, O., 2016. The Future Fight. *Seapower*, March, pp. 14-17.

Kremer, J. e. M. B., 2014. *Cyberspace and International Relations,* Berlin: Springer.

Lopes, J., 2016. *Intervenção do Ministro da Defesa Nacional na conferência A Cimeira da NATO em Varsóvia e o novo ambiente de segurança internacional.* Lisboa, Gabinete do Ministro da Defesa Nacional, p. 12.

Maquiavel, N., 1976. *O Príncipe.* Mem Martins, Publicações Europa-América.

Marques, A., 2017. *O Poder da Informação no Poder Militar (Conferência ao CPOG 2016-2017, em 2017-02-21).* Lisboa, IUM.

MDN, 2013. Orientação política para a ciberdefesa (Despacho n.º 13692/2013). *Diário da República, 2ª série - N.º 208*, 28 outubro, pp. 31977-31979.

MDN, 2014a. *Missões das Forças Armadas MIFA 2014 (CSDN de 30 de julho).* Lisboa: MDN.

MDN, 2014b. Diretiva Ministerial de Planeamento de Defesa Militar (Despacho n.º 11400/2014). *Diário da República, 2.ª série — N.º 175*, 11 setembro, pp. 23656-23657.

MDN, 2014g. Diretiva Ministerial de Planeamento de Defesa Militar (Despacho n.º 11400/2014). *Diário da República, 2.ª série — N.º 175*, 11 setembro, pp. 23656-23657.

NATO - CCD COE, 2015. *The Role of Offensive Cyber Operations in NATO's Collective Defence,* Tallinn: NATO - CCD COE.

New Zeland Government, 2015. *New Zeland's Cyber Security Strategy.* [Em linha] Disponível em: http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-december-2015.pdf
[Acedido em 2 3 2017].

Nunes, P. V., 2015. *Sociedade em Rede, Ciberespaço e Guerra da Informação. Contributos para o Enquadramnto e Construção de Uma Estratégia Nacional de Informação.* s.l.:Instituto da Defesa Nacional.

OTAN, 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge: Cambridge University Press.

OTAN, 2014a. *Enhanced NATO Policy on Cyber Defence (PO(2014)0358), 27 May,* Brussels: NATO.

OTAN, 2014b. *NATO Cyber Defence Taxonomy and Definitions.* Norfolk: Consultation, Command and control Board (NC3B).

OTAN, 2016a. *BI-SC Final assessment of recognising cyberspace as a domain (IMSWM-0190-2016),* s.l.: BI-SC.

OTAN, 2016b. *Military advice on the recognition of cyberspace as a domain (MCM-0083-2016),* Brussels: Military Committee.

OTAN, 2016c. *Warsaw Summit Communiqué (at NATO Portal).* [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber [Acedido em 12 02 2017].

OTAN, 2017. *AJP-3.20 Doctrine for Cyberspace Operations.* Version 1 (2017/01/26) ed. s.l.:OTAN.

Oxford University, 2017. *Oxford English Dictionary.* [Em linha] Disponível em: https://en.oxforddictionaries.com/definition/cyberspace [Acedido em 2 3 2017].

Rajnovic, D., 2012. *Cyberspace – What is it?,* San José, Califórnia, EUA: s.n.

Rocha, M., 2003. *Ciberdúvidas da Língua Portuguesa.* [Em linha] Disponível em: https://ciberduvidas.iscte-iul.pt/consultorio/perguntas/como-apareceu-a-palavra-cibernauta/15349 [Acedido em 21 02 2017].

Roodt, J., Oosthuizen, R. & Vuuren, J., 2015. *Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces.* s.l., Conference on Information Warfare & Security.

Schwab, K., 2016. *A Quarta Revolução Industrial.* s.l.:s.n.

Seffers, G., 2015b. U.S. Army Builds Cyber Branch One Step at a Time. *Signal*, April, pp. 38-41.

Shakarian, P. & Shakarian, J. e. R. A., 2013. *Introdution to Cyberwarfare.* Waltham, MA: Elsevier.

Sprong, E., 2016. *Dutch Cyber Strategy.* s.l., Ministry of Defence.

Strassmann, P., 2015. Cyberwarfar Needs More Brains. *Signal*, April, pp. 49-50.

Taylor, D. P., 2016. Force Multiplier: Navy looks to develop cyber capabilities as part of its air warfare domain. *Seapower*, October.

The Economist, 2010. *CYBERWAR: It is time for countries to start talking about arms control on the internet.* [Em linha]
Disponível em: http://www.economist.com/node/16481504
[Acedido em 10 novembro 2016].

The Netherlands Government, 2013. *National Cyber Security Strategy 2.* [Em linha] Available at: https://english.nctv.nl/binaries/national-cyber-security-strategy-2_tcm32-84265.pdf
[Acedido em 2 3 2017].

UE, 2013. *Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido [JOIN(2013) 1 final]*, Bruxelas: União Europeia.

UE, 2016. *EU Concept on Cyber Defence for EU-led Military Operations and Missions, Rev 2*, Brussels: EU Military Staff.

UK Government, 2016. *UK National Cyber Security Strategy 2016-2021.* [Em linha] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[Acedido em 2 3 2017].

US Cyber Command, 2015. *Beyond the Build, delivering Outcomes throuh Cyberspace: The Commaner's Vision and Guidance for US Cyber Command*, Fort Meade: Department of Defense.

US Department of Defense, 2016. *Joint Publication 1-02 - Dictionary of Military and Associated Terms.* USA: DoD.

US JCS, 2013. *JP 3-12(R) Cyberspace Operations*, Washington DC: United States Armed Forces Joint Chiefs of Staff.

Westphal, M., 2015d. Building a Capability Development Work Force For the Cyber Age. *Signal*, July, pp. 44-46.

Winston, B. & Patterson, K., n.d. *An Integrative Definition of Leadership.* [Em linha] Available at: https://www.regent.edu/acad/global/publications/ijls/new/vol1iss2/

winston_patterson.doc/winston_patterson.htm

[Acedido em 04 dezembro 2016].

Apêndice A — Corpo de Conceitos

Fazendo-se referência e uso de vários conceitos ao longo do presente TIG, de variadas fontes, apresentam-se de seguida esses mesmos conceitos, divididos em dois grupos: um primeiro relativo ao conceito de "ciberespaço" com apresentação de múltiplas fontes, e um segundo grupo com os outros conceitos que são referenciados ou utilizados ao longo do TIG.

- Capacidade militar: "o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade" (MDN, 2014g, p. 23657).
- Ciberataque: ato ou ação iniciada no ciberespaço para causar dano através do compromisso das comunicações da informação ou outros sistemas eletrónicos, ou da informação armazenada, processada ou transmitida nesses sistemas (OTAN, 2014b).

Conceitos referentes a "ciberespaço"

- Oxford English Dictionary (Oxford University, 2017):
  - *The notional environment in which communication over computer networks occurs*.

- Austrália (Australia Government, 2016):
  - *Cyber security refers to the safety of computer systems – also known as information and communications technologies (or ICT).*

- Canada, (Canada Government, 2010):
  - *Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.*

- The Netherlands (The Netherlands Government, 2013):
    - *Cyber security is to be free from danger or damage caused by disruption or fall-out of ICT or abuse of ICT. The danger or the damage due to abuse, disruption or fall-out can be comprised of a limitation of the availability and reliability of the ICT, breach of the confidentiality of information stored in ICT or damage to the integrity of that information.*

- Germany (Germany Government, 2011):
    - *Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.*

- New Zealand (New Zeland Government, 2015):
    - *The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.*

- United Kingdom (UK Government, 2016):
    - *Cyberspace is the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept.*

- United States of America (US JCS, 2013):
    - *A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Approved for incorporation into JP 1-02.).*

- ITU (ITU, 2008):
    - *Technologies, such as wireless networks and voice-over-IP (VoIP), extend the reach and scale of the Internet. In this regard, the cyber environment includes users, the Internet, the computing devices that are connected to it and all applications, services and systems that can*

be connected directly or indirectly to the Internet, and to the next generation network environment, the latter with public and private incarnations. Thus, with VoIP technology, a desk telephone is part of the cyber environment. However, even isolated devices can also be part of cyber environment if they can share information with connected computing devices through removable media. The cyber environment include the software that runs on computing devices, the stored (also transmitted) information on these devices or information that are generated by these devices. Installations and buildings that house the devices are also part of the cyber environment.

- ISO/IEC (ISO/IEC, 2011):
    - *The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*.

- OTAN Tallinn Manual (OTAN, 2013)
    - *The environment formed by physical and non-physical components, characterized by use of computers and the electro-magnetic spectrum to store, modify, and exchange data using computer networks.*

- OTAN Military advice on the recognition of cyberspace as a domain (OTAN, 2016b, p. 2).
    - Domínio global e virtual criado pela interligação de todas as redes de comunicações, informação e sistemas eletrónicos e a informação armazenada e processada ou transmitida nesses sistemas