INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR

2016/2017

TII

CIBERGUERRA E CIBERPAZ NAS NOVAS RELAÇÕES INTERNACIONAIS

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.

Carlos Eduardo Correia de Passos

CAP/TINF

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CIBERGUERRA E CIBERPAZ NAS NOVAS RELAÇÕES INTERNACIONAIS

CAP/TINF Carlos Eduardo Correia de Passos

Trabalho de Investigação Individual do CPOS

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CIBERGUERRA E CIBERPAZ NAS NOVAS RELAÇÕES INTERNACIONAIS

CAP/TINF Carlos Eduardo Correia de Passos

Trabalho de Investigação Individual do CPOS

Orientador: MAJ/JUR
Inês Isabel Vicente Caetano de Sousa Luís

Pedrouços 2017

Declaração de compromisso Antiplágio

Eu, Carlos Eduardo Correia de Passos, declaro por minha honra que o documento intitulado Ciberguerra e Ciberpaz nas novas Relações Internacionais corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do CPOS FA 2016/17 no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.
Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, 26 de junho de 2017

Carlos Eduardo Correia de Passos
CAP/TINF

Agradecimentos

Foi com a orientação, o apoio e a ajuda de várias pessoas que o presente trabalho conseguiu chegar a bom porto e por isso expresso toda a minha gratidão.

Primeiro, gostaria de começar por reconhecer, agradecer e enaltecer toda a preciosa, perspicaz e sempre célere orientação, ajuda e incentivo que a Major Inês Luís nunca deixou de humildemente me proporcionar. Terá para sempre o meu reconhecimento.

É com natural emoção e apreço que agradeço à minha família, são os meus verdadeiros pilares e merecem um agradecimento especial. Às flores do meu jardim, a minha esposa, Vera, que acompanhei nesta aventura e com quem partilhei as responsabilidades familiares e à minha filha, Joana, que soube sempre mostrar aquele sorriso maroto quando eu precisava. Aos meus pais e ao meu irmão que mesmo longe estiveram sempre perto de mim.

Agradeço também ao Tenente-coronel Mendes que inicialmente me aconselhou o caminho a seguir, ao Major Rêgo pela disponibilidade em fornecer informação pertinente para o trabalho e à ajuda que os entrevistados me souberam dar. O Major Farinha que nunca se negou a responder a solicitações e a indicar soluções e o Capitão-tenente Assunção pela informação que ambos partilharam comigo, o Major Raposo e o Major Leite pela atenção que tiveram comigo, o Major Valente com quem partilho uma amizade já longa, o Capitão-tenente Baptista das Neves e o Major Vinagreiro pelas preciosas opiniões.

Finalizo com uma palavra de apreço aos camaradas do curso pelo ambiente que proporcionaram, em especial ao Capitão Baptista da Costa, com quem a partilha de pontos de vista dos trabalhos de investigação foi importante.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

O dilema de qualificar como ato de ciberguerra um ciberataque não se limita a motivar atenção às questões do direito internacional, no âmbito de um mundo virtual. Um ato de ciberguerra tem implicações reais e diretas na vida dos cidadãos e a eventualidade da sua ocorrência obriga os Estados a munirem-se de capacidades de ciberdefesa.

Neste estudo do caso português, são conhecidas as capacidades da estrutura definida para a ciberdefesa nacional, avaliadas as valências e detetadas as vulnerabilidades do centro de ciberdefesa, através de um raciocínio indutivo, assente numa estratégia de investigação qualitativa.

O objetivo geral deste trabalho é avaliar as capacidades da atual estrutura definida para a ciberdefesa nacional.

Os seus objetivos específicos são: identificar a fronteira entre a ciberpaz e a ciberguerra; identificar os meios de que Portugal dispõe, na área da defesa, para exercer operações no ciberespaço; identificar aspetos a desenvolver na ciberdefesa nacional; propor recomendações para melhorar a atual capacidade da ciberdefesa nacional.

Este estudo permitiu concluir que a atual estrutura definida para a ciberdefesa nacional tem capacidade para exercer ciberoperações no contexto internacional, devendo haver um investimento no reforço de recursos humanos e na definição de doutrina.

Palavras-chave: ciberespaço, ciberataque, ciberguerra, ciberoperações, cibersegurança, ciberdefesa

Abstract

The dilemma of qualifying a cyberattack act as cyberwarfare is not limited to call one's attention to issues of international law within a virtual world. An act of cyberwar has real and direct implications on citizens' lives and the possibility of it happening compels States to equip themselves with cyberdefense capabilities.

In this Portuguese case study, the capabilities of the structure defined for national cyber defense are known, the valencies are evaluated and the vulnerabilities of the cyberdefense center are detected. It followed an inductive reasoning based on a qualitative research strategy.

The overall objective of this work is to evaluate the capabilities of the current framework defined for national cyberdefense.

Its specific objectives are: identifying the border between the cyberpeace and the cyberwar; identifying the tools/ways that Portugal has got, in the defense area, to carry out operations in cyberspace; identifying aspects to be developed in national cyber-defense; proposing recommendations to improve the current capacity of national cyber-defense.

This study determined that the current structure defined for national cyber-defense has the ability to exercise cyber operations in the international context, and there should be an investment in reinforcing human resources and define doctrine.

Keywords: *cyberspace, cyberattack, cyberwar, cyber operations, cybersecurity, cyberdefense*

Lista de abreviaturas, siglas e acrónimos

AED	Agência Europeia da Defesa
ANPC	Autoridade Nacional de Proteção Civil
AR	Assembleia da República
CCD	Centro de Ciberdefesa
CCDCOE	*Cooperative Cyber Defence Centre of Excellence*
CERT	*Computer Emergency Response Team*
CIRC	*Computer Incident Response Capability*
CNCS	Centro Nacional de Cibersegurança
CNU	Carta das Nações Unidas
CSIRT	*Computer Security Incident Response Team*
CPOS	Curso de Promoção a Oficial Superior
CUE	Conselho da União Europeia
EMGFA	Estado-Maior-General das Forças Armadas
ENISA	*European Union Agency for Network and Information Security*
EUA	Estados Unidos da América
EX	Exército
FA	Força Aérea
FFAA	Forças Armadas
GNR	Guarda Nacional Republicana
GNS	Gabinete Nacional de Segurança
IC	Infraestruturas Críticas
ICE	Infraestruturas Críticas Europeias
ICS	*Industrial Control Systems*
IESM	Instituto de Estudos Superiores Militares
ITU	*International Telecommunication Union*
IUM	Instituto Universitário Militar
MAR	Marinha
MDN	Ministério da Defesa Nacional
MoU	Memorando de Entendimento
NCIA	*Nato Communications and Information Agency*
NCIRC	*Nato Computer Incident Response Capability*

NIS	*Network and Information Security*
NU	Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PCM	Presidência do Conselho de Ministros
PD	Pergunta Derivada
PP	Pergunta de Partida
RFA	Regulamento da Força Aérea
RH	Recursos Humanos
SCADA	Sistemas de Supervisão e Aquisição de Dados
UE	União Europeia
USAWC	*United States Army War College*

Introdução

Ciberguerra

Quando a Utopia se Transforma em Realidade

(Fernandes, 2014)

Será possível imaginar que uma barragem hidroelétrica, sem controlo, comece a lançar grandes quantidades de água sobre localidades próximas, ou que gere eletricidade prejudicando a rede elétrica nacional, ou que os radares de aproximação dos aeroportos deixem de funcionar, ou que as aeronaves recebam informações erradas levando à queda das mesmas, ou que os sistemas bancários deixem de funcionar criando uma crise financeira, ou que os sinais de trânsito desliguem?

Será possível que estas situações aconteçam ao mesmo tempo?

Será possível imaginar que estas situações aconteçam em Portugal?

Infelizmente, estes eventos já não são tão difíceis de acontecer como imaginávamos.

Neste momento, a facilidade de atingir objetivos ao nível global é notoriamente possível, utilizando o espaço virtual - o ciberespaço, onde a ligação virtual entre o homem e o mundo apresenta oportunidades ao alcance de um clique.

As relações internacionais têm assim mais um espaço de diálogo, que se constitui como uma ferramenta de relevo, a ter em consideração. Com mais um espaço de diálogo, surgem mais oportunidades de expansão de poder e de influência na política mundial.

A história demonstra que a expansão de poder nem sempre acontece pacificamente. Quando a expansão de poder enfrenta oposição, ocorrem guerras, aumenta o crime.

Em abril de 2007, a Estónia foi alvo de ciberataques massivos durante 3 semanas (theguardian, 2007), inutilizando por algum tempo algumas infraestruturas críticas. Embora o ataque não tenha sido reivindicado, a Estónia acusou a Rússia de o ter perpetrado, em resposta à mudança de lugar da estátua do Soldado de bronze de Tallinn, uma estátua com significado especial para a Rússia.

No ano seguinte, na Guerra na Ossétia do Sul entre a Rússia e a Geórgia, a Rússia foi mais uma vez acusada de utilizar ciberataques, mas neste caso como complemento aos ataques convencionais (The New York Times, 2008).

Mais recentemente, em 2010, o ataque do sofisticado vírus “Stuxnet”, considerado como a primeira grande ciberarma, conseguiu danificar o projeto nuclear do Irão, assim como coexistir em diversos sistemas ao nível global (Daily Mail, 2010).

Assim, o ciberespaço surge como mais um domínio para fazer a guerra, para além dos tradicionais espaços terrestre, naval e aéreo. É por esta razão que a Organização do Tratado do Atlântico Norte (OTAN) designou o ciberespaço como um domínio operacional oficial de guerra (CCDCOE, 2016), que designou como ciberguerra.

Neste contexto, é cada vez mais premente para os Estados munirem-se de meios de controlo no âmbito da cibersegurança e da ciberdefesa.

Desta forma, justifica-se a necessidade de estudar as valências da atual estrutura definida para a ciberdefesa em Portugal, mais concretamente no caso de haver necessidade de exercer operações no ciberespaço no contexto internacional, ultrapassando a fronteira entre o que é a ciberpaz e a ciberguerra.

O objeto de estudo do trabalho de investigação é conhecer as capacidades da atual estrutura definida para a ciberdefesa nacional, avaliar essas valências e detetar as atuais vulnerabilidades do centro de ciberdefesa (CCD), apontando aspetos que poderão melhorar a ciberdefesa nacional.

O tema foi delimitado em três domínios distintos: tempo (atualidade), espaço (nacional) e conteúdo (capacidades de ciberdefesa). A avaliação das capacidades atuais, face ao que atualmente se sabe relativamente à ciberdefesa nacional, tem grande enfoque no CCD.

Deste modo, o objeto de estudo responde então às seguintes questões: Quem? (ciberdefesa nacional); O Quê? (as capacidades atuais); Onde? (CCD); Quando? (No contexto atual).

Tendo como objetivo geral da investigação a avaliação das capacidades da atual estrutura definida para a ciberdefesa nacional, mais especificamente através da identificação da fronteira entre a ciberpaz e a ciberguerra, e da identificação dos meios de que Portugal dispõe, na área da defesa, para exercer operações no ciberespaço e da identificação dos aspetos a desenvolver na ciberdefesa nacional, será possível propor recomendações para melhorar a atual capacidade da ciberdefesa nacional e responder às questões que surgem da necessidade de avaliar a atual capacidade da estrutura definida para a ciberdefesa nacional, permitindo assim aferir as suas valências e as vulnerabilidades no contexto internacional.

Assim, a pergunta de partida (PP) deste trabalho é: A atual estrutura definida para a ciberdefesa nacional tem capacidade para exercer ciberoperações no contexto internacional?

O trabalho foi desenvolvido segundo um raciocínio indutivo, assente numa estratégia de investigação qualitativa, em que é efetuado um estudo de caso fundamentado com análise documental e entrevistas semiestruturadas que se encontram no Apêndice H.

Estruturalmente, o trabalho de investigação será baseado na NEP/ACA – 018 de setembro de 2015 do Instituto de Estudos Superiores Militares (IESM) e será dividido em três partes: introdução, corpo e conclusão (2015a, p. 4).

O corpo do trabalho é constituído por 3 capítulos.

1. Exposição da metodologia de investigação, onde é exposto o modelo de análise e justificada a razão da sua implementação;
2. Investigação propriamente dita, com grande enfoque em revisão literária com auxílio de entrevistas semiestruturadas, em que a ameaça cibernética é caraterizada no seu espaço de manobra – o ciberespaço, onde são abordados aspetos da ciberguerra, cibersegurança e da ciberdefesa;
3. Análise da informação recolhida no estudo, dando resposta às perguntas derivadas.

Nas conclusões do trabalho, será realizado um sumário das linhas do procedimento metodológico adotado, serão avaliados os resultados obtidos em relação aos objetivos estabelecidos, salientados alguns contributos, recomendações e limitações.

1. Resumo da Literatura, Modelo de Análise e Metodologia

1.1. Resumo da Literatura

Para consubstanciar a teoria desenvolvida neste trabalho foi necessário consultar um leque alargado de documentos e trabalhos realizados nesta área.

Inicialmente foi empregue um esforço em trabalhos que posicionassem e delimitassem a informação necessária para realizar um trabalho robusto.

Foram consultados livros e documentos que caraterizassem o ambiente em que o contexto de trabalho se enquadra – o ciberespaço, onde foi identificada doutrina, documentos oficiais e documentos de trabalho. De seguida, foi necessário consultar informação jurídica, militar e documentos narrativos de casos de estudo para fundamentar o contexto da ciberguerra. Por fim, foram consultados estudos sobre o poder cibernético, documentos estruturantes e trabalhos sobre as políticas da OTAN, União Europeia (UE), Nações Unidas (NU) e da implementação nacional para entender a necessidade de edificação da capacidade de ciberdefesa.

1.2. Modelo de Análise

A PP do trabalho tem como objetivo saber se a atual estrutura definida para a ciberdefesa nacional tem capacidade para exercer ciberoperações no contexto internacional. As respostas às perguntas derivadas (PD) são necessárias para dar robustez à PP. As PD são as seguintes:

PD 1 - Existe presentemente necessidade de dotar Portugal de capacidades para operar em contexto de ciberguerra?

PD 2 - O CCD tem os meios necessários para exercer ciberoperações?

PD 3 - Existem capacidades que merecem ser melhoradas para dotar o CCD de uma capacidade relevante para operar no contexto internacional?

O trabalho estará delimitado às capacidades atuais da ciberdefesa nacional.

Deste modo, a investigação terá como base a observação da atual estrutura definida para a ciberdefesa nacional. Na sequência da observação realizada, serão induzidos conceitos, desdobrados em dimensões, conforme sumarizado no Apêndice A. É de realçar que num estudo qualitativo as variáveis não carecem de caráter mensurável (Bryman, 2012, p. 48).

1.3. **Metodologia**

Foi aplicado o raciocínio indutivo, pois segundo o Instituto Universitário Militar (IUM) "(…) corresponde a uma operação mental que tem como ponto de partida a observação de factos particulares para, através da sua associação, estabelecer generalizações que permitem formular uma lei ou teoria" (2016, p. 20).

O desenvolvimento ficou assente numa estratégia de investigação qualitativa, em que "(…) existe uma relação indissociável entre o mundo real e a subjetividade do sujeito, que não é passível de ser traduzida em números (…)", cujos "(…) estudos são essencialmente indutivos e descritivos (…)" (IUM, 2016, p. 29) e que "(…) o seu objetivo passa normalmente pela compreensão do significado atribuído por um individuo ou por um grupo(…)" (Creswell, 2013, p. 4 cit. IUM, 2016, p. 29).

Quanto ao desenho de pesquisa utilizado, a temática apresentada enquadra-se num estudo de caso, nomeadamente, a atual estrutura definida para a ciberdefesa nacional, com grande enfoque no CCD. De facto, o estudo de caso procura "recolher informação sobre um fenómeno particular inserido no seu contexto" (Saunders et all., 2009, p.145 cit IUM, 2016, p. 39). É um desenho de pesquisa "(…) tendencialmente enquadrado no âmbito das estratégias de investigação qualitativas, apresentando uma natureza essencialmente empírica e descritiva (…)" (IUM, 2016, p. 39), onde as técnicas de recolha de dados utilizadas foram a análise documental e as entrevistas semiestruturadas.

Baseando-se no indicado no pt. 5 da NEP/ACA-010, de 15 de setembro de 2015 (IESM, 2015b), o percurso metodológico seguido neste trabalho de investigação passou inicialmente por uma fase exploratória, onde se teve um primeiro contacto com o tema, posteriormente por uma fase analítica, onde foram analisados os dados associados à temática apresentada e finalmente uma fase conclusiva, onde foram apresentadas conclusões e recomendações acerca do trabalho.

2. Ameaça Cibernética

Nos últimos anos, o número de ataques cibernéticos tem aumentado, alguns casos mediáticos como os ataques à Estónia, Geórgia e o vírus "Stuxnet" chegaram mesmo a roçar o limiar da fronteira entre a ciberpaz e a ciberguerra.

Todos estes acontecimentos decorrem da recente ameaça, a ameaça cibernética, onde o perigo é latente, real e comprovado com factos recentes e cuja existência se deve ao recente espaço – o ciberespaço.

2.1. Ciberespaço

"A utilização deste espaço de natureza virtual apresenta potencialidades que ninguém ousara visionar, permitindo que atores políticos, económicos, religiosos e os que se dedicam à prática do crime se possam confrontar a nível global, tanto em termos competitivos como conflituais, com armas potencialmente letais ou não." (Santos, 2014)

Se recorrermos ao Manual de Tallinn (CCDCOE, 2009, p. 258), ciberespaço é o "ambiente formado por componentes físicos e não físicos, caraterizado pelo uso de computadores e espectro eletromagnético, para armazenar, modificar e trocar dados usando redes de computadores"[1]. De um modo mais genérico, o ciberespaço "é mais do que a internet, incluindo não só hardware, software e sistemas de informação, mas também pessoas e interação social dentro dessas redes"[1], (Klimburg, 2012).

Uma outra forma de definir o ciberespaço, é caraterizá-lo quanto ao contexto e propósito que é utilizado, (Clark, 2010). As caraterísticas estão descritas no Apêndice B, a Figura 1 exemplifica as camadas (níveis) com legendas sobre os componentes e os objetos.

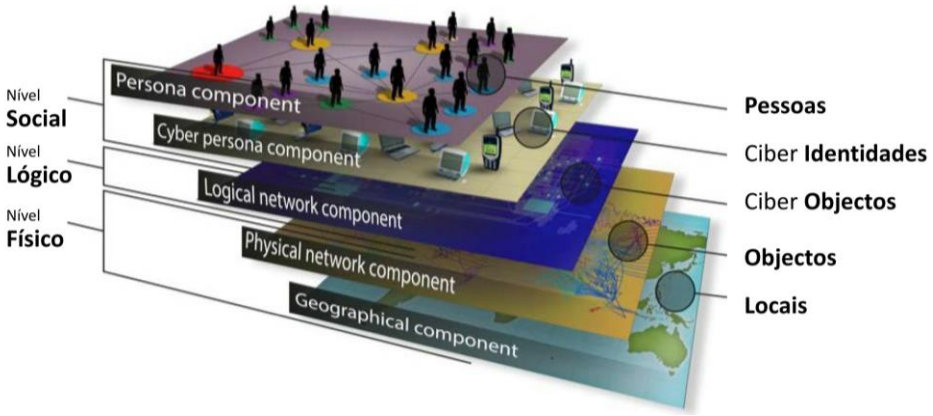

Figura 1 - Camadas/Níveis do Ciberespaço

Fonte: (Silva, 2016, p. 6)

[1] Tradução do autor.

No Apêndice B estão especificadas as particularidades do ciberespaço:

- Pode ter a capacidade de engenharia reversa;
- Não é propriedade nacional ou internacional;
- Falta de cooperação ou colaboração internacional;
- Baixo custo;
- Volátil;
- Rápida;
- Efeitos em cascata não intencionais;

Segundo o Coronel Paulo Viegas Nunes (2016, p. 52) as sociedades mais desenvolvidas usam o ciberespaço como caraterística fundamental para a implementação dos sistemas, onde empresas multinacionais se tornam supranacionais e assim capazes de ter poder de influência em poderes nacionais. É assim que o Coronel Paulo Viegas Nunes identifica a sociedade em rede, um sistema de sistemas, e está exemplificado na Figura 2.

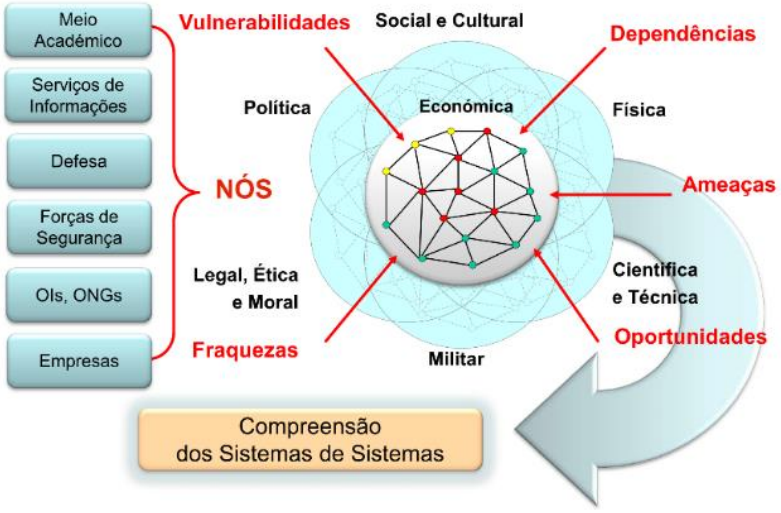

Figura 2 - Sistema de sistemas no ciberespaço

Fonte: (Grossman-Vermaas, 2004 cit. Nunes, 2016, p. 53)

O ciberespaço é assim um espaço de progresso apetecível, mas do mesmo modo que cria oportunidades, evidencia as vulnerabilidades, pois quanto maior a exposição, maior o risco.

2.1.1. Vulnerabilidades

É neste contexto que se enquadram as infraestruturas críticas (IC). Segundo o Ministério da Defesa Nacional (MDN) (2011), uma infraestrutura crítica é "(…) a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada

a impossibilidade de continuar a assegurar essas funções (…)". A preocupação com a segurança das IC está latente na definição elaborada pela Autoridade Nacional de Proteção Civil (ANPC) (2016), considerando que uma infraestrutura crítica é aquela "(…) que, caso sofra uma disfunção, pode por em causa o funcionamento do país e o bem-estar da sua população".

No intuito de melhorar a proteção das infraestruturas críticas europeias (ICE), foi aprovada a Diretiva 2008/114/CE do Conselho da União Europeia (CUE), que estabelece os procedimentos para identificar as ICE. Nesta diretiva estão identificados os vários setores em que se enquadram as ICE (CUE, 2008), conforme exemplificado na Tabela 1.

Tabela 1 - Lista de setores de enquadramento das ICE

Sector	Subsetor	
I Energia	1. Eletricidade	Infraestruturas e instalações de produção de transporte de eletricidade, em termos de abastecimento
	2. Petróleo	Produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos
	3. Gás	Produção, refinação, tratamento, armazenagem e transporte de gás, por gasodutos Terminais para GNL
II Transportes	4. Transportes rodoviários	
	5. Transportes ferroviários	
	6. Transportes aéreos	
	7. Transporte por vias navegáveis interiores	
	8. Transporte marítimo, transporte marítimo de curta distância e portos	

Fonte: (CUE, 2008)

A Diretiva 2008/114/CE do CUE foi transposta para a ordem jurídica portuguesa através do Decreto-Lei nº 62/2011.

Segundo o Coronel Paulo Viegas Nunes (2016, pp. 127-130), com o ciberespaço as vulnerabilidades das IC foram ampliadas, devendo ser considerado um modelo de interdependência das IC nacionais, que para além das IC deve incluir infraestruturas de risco, concretamente as redes de comunicações, o sistema financeiro, a defesa, a proteção civil, e pilares estruturantes da sociedade como o governo, a saúde, o sistema de distribuição de água, que caso sejam afetadas têm impacto significativo no bem-estar das populações.

As IC "(…) utilizam os Sistemas de Controlo Industrial (ICS – *Industrial Control Systems*) para a gestão e a monitorização dos correspondentes processos. Estes ICS têm passado por uma transformação significativa nos últimos anos, passando de sistemas autónomos de tecnologias proprietárias para arquiteturas abertas, altamente interligadas com sistemas corporativos e inclusive com a internet" (IDN-CESEDEN, 2013, p. 18).

Segundo a *European Union Agency for Network and Information Security* (ENISA) (2015) os ICS permitiram reduzir custos, melhorar a usabilidade, monitorizar vários processos e aceder remotamente, tornando as IC mais vulneráveis a ataques. O Sistema de Supervisão e Aquisição de Dados (SCADA) é o ICS mais representativo. O SCADA fornece indicadores para tomadas de decisão e identifica problemas, o que aumenta a eficiência (Inductive Automation, 2016).

Desta forma, as ICS estão vulneráveis a ciberataques. O Regulamento da Força Aérea (FA), RFA 390-6 (2011) define ciberataque como "uma das formas que pode tomar a Ciberguerra", e que poderá "ser combinada com um ataque físico ou não, e destina-se a provocar danos na capacidade dos sistemas". O entrevistado Major Raposo, afirmou que a salvaguarda das nossas IC enquadra-se na exigência de comportamentos e medidas de segurança, sendo alvo de atenção especial (2017).

Todas as possibilidades de ciberataques são uma ameaça. As ameaças provenientes do ciberespaço são as ciberameaças - ação "perpetrada através da Internet ou de outra rede de computadores com objectivo de intrusão ou acesso ilegal" (Dicionário Priberam da Língua Portuguesa, 2008a).

2.1.2. Ameaças

As ameaças "(…) são hoje assimétricas com uma multiplicidade enorme de actores, desde indivíduos a grupos organizados ou mesmo Estados hostis possuindo um largo espectro de motivações que poderão ser de carácter religioso, financeiro ou político, entre outros" (FA, 2011). No Apêndice C estão enunciados os diversos aspetos que caracterizam as ameaças cibernéticas, nomeadamente:

- A importância que ameaças cibernéticas têm nas estratégias de ataque de diversos atores;
- O grande investimento que potenciais adversários têm realizado no ciberespaço, concretamente a Rússia e a China, mas também onde Estados como o Irão e a Coreia do Norte têm investido, potenciando o poder militar, aproveitando o baixo custo relativamente a outras vertentes de cariz ofensivo, como ilustrado na Figura 3.

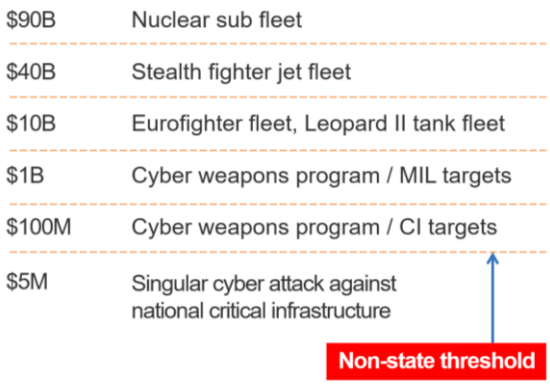

Figura 3 - Economia Militar

Fonte: (Langner, 2012)

- Diversidade de atores.

No caso nacional, o Major Raposo, confirmou que a ameaça é "(…) real, mas não completamente desconhecida (…)", sendo que dificilmente se irá saber dos casos em que as entidades resolvem as situações internamente (2017). Da entrevista efetuada no CCD, concretamente ao Major Farinha e ao Capitão-tenente Assunção, o nível de ameaça às Forças Armadas (FFAA) é médio (Farinha & Assunção, 2017).

"Em Portugal, 25% das empresas participantes no Estudo da Marsh, admitiram ter sido alvo de um ataque cibernético (…)" em 2016, "(…) assim como 38% identifica o risco cibernético no Top 5 dos seus riscos corporativos." (PCguia, 2016).

2.2. **Cibercrime e ciberguerra**

Nos termos do n.º 1 do artigo 29.º da Constituição da República Portuguesa (AR, 2005), ninguém pode ser sentenciado criminalmente senão em virtude de lei anterior que declare punível a ação ou a omissão. Este preceito consagra o princípio *nullum crimen, nulla poena sine lege*, ou seja, princípio de que não há crime nem pena sem lei.

Ou seja, uma conduta constitui-se como prática ou omissão de crime se, nos termos da lei, for qualificada como criminosa (Palma, 2012).

Neste sentido, concorda-se com Solange Ghernaouti (2013, p. 149), quando refere que a problemática do cibercrime está relacionada "com o cumprimento da lei e os sistemas judiciais e da justiça e da segurança interna"[2].

[2] Tradução do autor.

Ora, no que concerne ao ciberespaço, o cibercrime e as ações de ciberguerra usam os mesmos meios e as mesmas aptidões humanas, onde os ciberataques são um denominador comum.

Desta forma, para muitos autores, a ciberpaz tem uma fronteira ténue com a ciberguerra. Richard A. Clarke[3] e Robert K. Knake descrevem em *Cyber War The Next Threat to National Security and What to Do About It* (2010, p. 64), que o Estado norte-americano passaria do ambiente de ciberpaz para o estado de ciberguerra quando as suas IC fossem alvo de ciberataques externos e por consequência começassem a falhar, dando por exemplo o surgimento de incêndios e explosões nas refinarias, a libertação de nuvens de cloro por empresas de produtos químicos, entre outros.

Atualmente, ainda não existe consenso sobre quando uma ação cibernética é considerada um ato de ciberguerra. Estão inclusive identificadas várias abordagens à diferenciação de ato de ciberguerra, cibercrime, ciberespionagem, ciberterrorismo e ciberactivismo (PCWorld, 2012).

- Richard Stiennon, (Analista Chefe de Investigação da IT-Harvest), defende "(…) que é preciso uma investigação mais profunda sobre os objetivos e os motivos do ataque para lhe atribuir um rótulo (…)"[4] (2012) e diferencia os vários grupos de ciberameaças.
- Mike Reagan, (Diretor de Marketing da empresa de segurança de informação, LogRhythm), "(…) acredita que as linhas estão definitivamente a ficar desfocadas, mas a distinção importa em termos de definir se um incidente é da responsabilidade da aplicação da lei ou dos militares (…)"[4] (2012), no contexto da fronteira entre a ciberpaz e a ciberguerra.
- Andrew Storms, (Diretor de Operações de Segurança da empresa de segurança em redes de computadores, ncircle), sugere remover os prefixos cyber "(…) e aplicar o mesmo julgamento usado em outros contextos (…)"[4] (2012), isto é, usando as leis atuais aplicadas às atividades no ciberespaço.
- Alex Seger, (Chefe da Divisão de Criminalidade Económica do Conselho Europeu), "(…) diz que, em vez de se concentrar nas definições, devemo-nos concentrar nos ataques: metodologias, metas e consequências (…)"[4] (2012).

[3] "(…) RICHARD A. CLARKE prestou serviço na Casa Branca para os presidentes Ronald Reagan, George H.W. Bush, George W. Bush e Bill Clinton, que o nomearam como Coordenador Nacional de Segurança, Proteção de Infra-estruturas e Contra-Terrorismo (…)"[4] (Clarke & Knake, 2010).

[4] Tradução do autor.

Depois de apresentadas várias abordagens, é pertinente esclarecer alguns aspetos relativos ao Direito Internacional Humanitário, de modo a responder a algumas dúvidas de ordem jurídica relativamente ao contexto da ciberguerra.

O direito à guerra (*Jus ad bellum*) e o direito na guerra (*Jus in Bellum*) têm sido alvo de estudo desde há muitos anos. Cícero (106 AC – 46 AC), Santo Agostinho (354 - 430), São Tomás de Aquino (1225 – 1274) e Hugo Grócio (1583 - 1645), foram responsáveis por trabalhos notáveis nessa área. Atualmente, muitos são os autores que abordam a dúvida da legalidade do uso da força relacionada com operações cibernéticas.

O Manual de Tallinn, sendo um manual académico, mas doutrinário, tal como referido pelo entrevistado Major Leite (2017), aborda as questões jurídicas de modo a aplicar às operações cibernéticas a Lei Internacional, concretamente a lei na cibersegurança internacional e a lei dos conflitos cibernéticos. Está explícito neste manual que não há vazio jurídico nas matérias relacionadas com as operações cibernéticas, assim como que os peritos são unânimes em afirmar que a Lei Internacional existente se aplica às operações cibernéticas (CCDCOE, 2009, p. 5).

Tal como defendido pelos peritos que elaboraram o Manual de Tallinn, também o grupo governamental de peritos das Nações Unidas (NU) sobre os desenvolvimentos no domínio da informação e das telecomunicações no contexto da segurança internacional, chegou em 2013 ao consenso sobre a aplicabilidade do direito internacional ao ciberespaço, concretamente da Carta das Nações Unidas (CNU) (CCDCOE, 2015). Este é também o entendimento do Major Leite (2017).

Deste modo, os Estados podem recorrer a ações de ciberdefesa desde que as situações estejam enquadradas nos critérios do direito à guerra, patentes no Capítulo VII[5] da CNU, mais concretamente no artigo 51.º sobre a legítima defesa e no artigo 42.º, nos termos do qual o Conselho de Segurança pode decretar medidas militares (NU, 1945, pp. 9, 10 e 11).

No Manual de Tallinn, através da aplicação das operações cibernéticas à Lei Internacional, "(…) uma operação cibernética constitui um uso da força quando a sua escala e efeitos são comparáveis a operações não-cibernéticas que se elevam ao nível do uso da força (…)"[6] (2009, p. 45), onde escala e efeitos são referentes à quantidade e qualidade dos fatores a analisar para caraterizar o uso da força.

[5] Capítulo VII – Ação em caso de ameaça à paz, rutura da paz e ato de agressão (NU, 1945, p. 9).
[6] Tradução do autor.

Convém, deste modo, esclarecer a diferença entre uso da força e ataque armado. A dificuldade em distinguir ataque armado de uso da força está patente no artigo de Katharina Ziolkowski (2012). Michael N. Schmitt[7] (2012) esforça-se por esclarecer esta diferença, realçando o artigo 2.º (4) da CNU, sobre a proibição aos Estados de recorrerem à ameaça ou ao uso da força (NU, 1945, p. 3) e o artigo 51.º, sobre a legítima defesa em caso de ocorrência de ataque armado.

Os conceitos "uso da força" e "ataque armado" surgem em ambos os preceitos, mas Michael N. Schmitt distingue-os salientando uma ressalva no caso da Nicarágua[8], onde existem "(…) medidas que não constituem um ataque armado, mas que, no entanto, podem envolver o Uso da força"[9] (International Court of Justice, 1986, p. 100 cit Schmitt, 2012, p. 313), isto é, "(…) é necessário diferenciar as formas mais graves do uso da força de outras formas menos graves"[9] (2012, p. 313). É deste modo que se justifica a referência ao caso da Nicarágua pelo Manual Tallinn, onde o uso da força por um ator não estatal enviado, ajudado ou a agir em nome de um ator estatal, com o propósito de efetuar o ataque, a este ator estatal pode ser atribuída a responsabilidade da operação (2009, p. 56 e 57).

De qualquer modo, a qualificação do uso da força não reúne consenso na interpretação internacional. José Pedro Teixeira Fernandes (2014) aborda este problema e refere alguns métodos que podem constituir um padrão para classificar o uso da força, mas enfatiza que face à falta do consenso, os Estados irão efetuar uma classificação consoante o próprio entendimento.

Um dos métodos abordados por José Pedro Teixeira Fernandes é o critério de Michael N. Schmitt (1999), que permite "(…) avaliar em que medida um ciberataque poderá ser considerado um ataque armado, destrinçando-o, nomeadamente, de atos de coerção económica e/ou política" (Fernandes, 2014). Nesse critério, referido também por Katharina Ziolkowski (2012) como o "*Schmitt Criteria*", Michael N. Schmitt defende seis requisitos: gravidade, iminência, caráter direto, caráter invasor ou intrusivo, mensuralidade ou extensão e presumível legitimidade.

[7] Michael N. Schmitt, tem realizado trabalhos notáveis nas questões relacionadas com a aplicação das leis internacionais ao ciberespaço, onde é enaltecido o desenvolvimento do critério para decisão se um ciberataque constitui o uso da força (Schmitt, 1999), (conhecido como o "*Schmitt Criteria*"), e o trabalho como diretor do projeto do Manual de Tallinn (CCDCOE, 2009).

[8] O caso da Nicarágua ficou conhecido pela decisão do Tribunal Internacional de Justiça a favor da Nicarágua e contra os Estados Unidos da América (EUA), por ter violado as leis internacionais ao apoiar a rebelião contra o Estado da Nicarágua (International Court of Justice, 1986).

[9] Tradução do autor.

Pese embora a tese de a Lei Internacional existente se aplicar às operações cibernéticas ser sobejamente defendida, há desafios adicionais que limitam a aplicação jurídica às operações cibernéticas. O avanço da tecnologia permite que as operações cibernéticas não necessitem de proximidade com o objetivo, permitindo assim que tenham origem em locais remotos dos locais onde se pretende que haja efeito, o que limita a deteção de um ciberataque, a atribuição da responsabilidade dos ciberataques e a descoberta da origem dos mesmos, mais concretamente a identificação do ator responsável, o que requer a sinergia com organizações não ligadas ao ciberespaço para a análise dessas operações (Joint Publication 3-12 (R), 2013, pp. I-7).

Para melhor perceber quais os tipos de ciberataques ou operações cibernéticas cuja qualificação como cibercrime ou ciberguerra poderão ser objeto de debate judicial, estão definidas no Apêndice D as operações no ciberespaço – as ciberoperações.

2.3. **Cibersegurança e ciberdefesa**

A qualificação de um ato cibernético como cibercrime ou ciberguerra releva para efeitos de definir a instância correta para o respetivo combate e prevenção. Para este efeito, importa agora destrinçar os conceitos de cibersegurança e ciberdefesa.

Na "(…) cibersegurança incluem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco o espaço de liberdade individual/coletiva e de prosperidade que ele constitui e cuja responsabilidade de policiamento deve caber às Forças de Segurança e aos Serviços de Informações" (Ralo, 2013). Ou seja, a cibersegurança combate o cibercrime, o hacktivismo, a ciberespionagem e o ciberterrorismo (Nunes, 2016, p. 343).

Por "(…) ciberdefesa entendem-se as atividades de monitorização, prevenção e resposta às ameaças que ponham em risco a soberania e a segurança nacional (ciberguerra) e cuja responsabilidade de resposta recai nas Forças Armadas " (Ralo, 2013). A ciberdefesa ultrapassa, assim, o limiar da paz e tem como campo de atuação primordial, a ciberguerra.

2.3.1. Cibersegurança

Com o aumento dos incidentes, o alarme sobre a perturbação que os mesmos poderiam criar nas ICE fez disparar a necessidade de criar uma estratégia para a cibersegurança na UE, o que veio a acontecer em 2013 (Comissão Europeia, 2013).

No seguimento da definição da estratégia para a cibersegurança na UE e constatando que a UE não dispunha de capacidades "(…) suficientes para garantir um elevado nível de segurança das redes e dos sistemas de informação (…)"[10], foi elaborada a diretiva *Network and Information Security* (NIS) (CUE, 2016).

O Major Raposo enfatizou a diretiva NIS, que determinou a criação da rede europeia de *Computer Security Incident Response Team* (CSIRT), composta por CSIRT dos Estados-Membros (2017). As CSIRT também são conhecidas por *Computer Emergency Response Team* (CERT) (CUE, 2016).

De modo a preparar-se para as ciberameaças e seguindo diretrizes da UE, Portugal avançou com um Conceito Estratégico Nacional.

No ano de 2014, foi regulamentado pela Presidência do Conselho de Ministros (PCM) o Centro Nacional de Cibersegurança (CNCS) a funcionar no Gabinete Nacional de Segurança (GNS) (2014).

O CNCS tem como missão "(...) contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais (…)" (PCM , 2014).

No CNCS está integrado o CERT.PT, que está identificado como um serviço "(…) que coordena a resposta a incidentes envolvendo entidades do Estado, operadores de serviços essenciais e prestadores de serviços digitais e, de uma forma geral, o ciberespaço nacional, incluindo qualquer dispositivo pertencente a uma rede ou bloco de endereçamento atribuído a um operador de comunicações eletrónicas, instituição, pessoa coletiva ou singular com sede em território Português, ou que esteja fisicamente localizado em território Português(…)" (CNCS, 2016a).

[10] Tradução do autor.

O Estado-Maior-General das Forças Armadas (EMGFA) é desde 2008 membro da rede nacional de CSIRT (Centro Nacional de Cibersegurança, 2016b), coordenada pelo CERT.PT.

O CNCS contribui também para a "formação de uma comunidade de conhecimento e uma cultura nacional de cibersegurança" (PCM , 2014), neste sentido a "formação escolar ao nível académico não superior é uma vertente que é também explorada" (Raposo, 2017).

2.3.2. Ciberdefesa

No ciberespaço surgiu mais um espaço de oportunidade de exercer poder, nomeadamente, poder militar. Embora a definição de ciberguerra ainda esteja a ser trabalhada, conforme referido, a verdade é que já estão identificados alguns ataques cibernéticos, demonstrados no Apêndice E, que foram tornados públicos e cuja qualificação entre cibersegurança e a ciberdefesa se afigura complexa.

Estes casos têm em comum o facto de os ataques terem sido perpetuados contra sistemas estatais, mas face à dificuldade em atribuir a responsabilidade dos ataques, não é possível afirmar que os responsáveis são Estados.

Estes conflitos demonstram a necessidade que os Estados têm de se munir de capacidades para exercer operações no ciberespaço, pois existe "em qualquer país, o potencial de acontecerem ataques como os registados" (Farinha & Assunção, 2017). É neste contexto que se enquadram os esforços empreendidos na criação de unidades de ciberdefesa.

A preocupação sobre o aproveitamento ameaçador e conflitual por parte de diversos atores levou a que Estados e organizações internacionais se precavessem, criando infraestruturas com o objetivo de agir usando o ciberespaço.

2.3.2.1. Plano internacional

Os Estados não pretendem ver as suas capacidades cibernéticas publicitadas, aumentando o poder de dissuasão e escondendo possíveis vulnerabilidades.

Há estudos que indicam o poder cibernético entre Estados ou organizações, através de cálculos efetuados com origem em variáveis ou até mesmo em opiniões de pessoas credíveis e com experiência no assunto, estão demonstrados no Apêndice F.

Estes estudos refletem as estratégias que alguns países empreenderam em capacidades no ciberespaço.

As capacidades de ciberdefesa dos países mais pontuados dos estudos abordados não estão todas edificadas do mesmo modo.

Alguns países criaram cibercomandos de modo a capacitar as FFAA de maior poder militar e poder de dissuasão, "(…) dos quais se salientam: EUA, Reino Unido, China, Rússia, Irão, Índia, Paquistão, Coreia do Norte, Coreia do Sul, Israel e, muitos mais" (IDN-CESEDEN, 2013, p. 36).

Em 2009, os EUA edificaram o *United States Cyber Command* (USCYBERCOM), um comando conjunto, com a missão de defender as redes e os sistemas de informação do departamento de defesa, aumentando a sua resiliência, e conduzir operações no ciberespaço, garantindo a liberdade de ação e privando a mesma aos adversários (Anon., 2016). Deste modo, investiram num comando robusto, cujo orçamento para operações no ciberespaço para 2017 rondará os 6,7 biliões de dólares (United States Department of Defense, 2016, pp. 5-5), com cerca de 6000 militares (Nextgov, 2016).

A abordagem chinesa é um pouco diferente. O facto de ser o país mais populoso, confere hipoteticamente um potencial de *hackers* elevado, que "(…) podem ser recrutados ou mobilizados para objetivos estratégicos e de interesse nacional (…)". Desde 2003 que o Exército de Libertação Popular da China tem unidades preparadas para ações de ciberguerra, que integram militares e *hackers* civis (Fernandes, 2014, pp. 119-120), num total até cerca de 100000 efetivos (The Washington Times, 2016).

A Rússia patrocina direta ou indiretamente atores não estatais para ações no ciberespaço. Há inclusive a suspeita do seu uso nos casos da Estónia e da Geórgia (Fernandes, 2014, pp. 121-122).

A Estónia empreendeu um modelo inovador, chamado "*Cyber Defence League*", que segundo o Major Leite utiliza "(…) as aptidões dos civis que estão a trabalhar durante o ano no privado, mas que se for necessário estão à disposição do interesse nacional" (2017).

As organizações internacionais também têm demonstrado iniciativas de empreenderem as mesmas capacidades, como está patente no Apêndice G, com as iniciativas da OTAN e da UE e como as NU têm empreendido tentativas frágeis para regulamentar o ciberespaço, pois segundo o Coronel Paulo Viegas Nunes "não há soluções locais para problemas globais" (Nunes, 2017). Na mesma senda, o jornalista Pedro Miguel Oliveira (Expresso, 2017) aborda iniciativas de organizações, como a da "Microsoft", com o objetivo de proteger utilizadores e dispositivos que usem a internet, que preconiza a criação de uma Convenção de Genebra Digital e defende que é necessário que

organizações internacionais criem algo como as "Nações Unidas Digitais", que estejam municiadas de uma força de "capacetes azuis virtuais" capazes agir em caso de ciberataques.

2.3.2.2. Plano Nacional

No contexto nacional, visando a melhoria das capacidades militares nacionais, foi aprovado o Conceito Estratégico de Defesa Nacional 2013, através da Resolução do Conselho de Ministros n.º 19/2013, que estabelece o levantamento da capacidade de ciberdefesa nacional (PCM, 2013). Ainda no mesmo ano, foi também definida a orientação política para a ciberdefesa (MDN, 2013).

No Decreto-Lei 184/2014, a estrutura do EMGFA compreende o CCD, mais concretamente na Direção de Comunicações e Sistemas de Informação (DIRCSI) (MDN, 2014).

O CCD é o centro empreendedor da política de ciberdefesa (MDN, 2013), e tem os seguintes objetivos definidos na orientação política para a ciberdefesa:

- "Garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques";
- "Assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional";
- "Contribuir de forma cooperativa para a cibersegurança nacional", com competências no âmbito da cibersegurança setorial.

No âmbito da interoperabilidade, está plasmado no Decreto Regulamentar 13/2015, que o CCD tem de assegurar "(…) a coordenação e o trabalho colaborativo e integrado com os núcleos *Computer Incident Response Capability* (CIRC) dos ramos das Forças Armadas e do EMGFA(…)", assim como partilhar "(…) a informação numa estratégia de resposta defensiva e colaborativa com o (…)" CNCS, as CIRC nacionais e internacionais, onde o *Nato Computer Incident Response Capability* (NCIRC) da OTAN se enquadra (MDN, 2015).

Esta interoperabilidade é salientada pelo Major Valente e o Major Vinagreiro, com realce para as sinergias e as experiências que resultam dos exercícios (Valente, 2017) (Vinagreiro, 2017), mas o Capitão-tenente Baptista das Neves verifica que a falta de doutrina conjunta dificulta, sendo necessário edificar "uma doutrina que enquadre a capacidade e uma organização que a suporte" (2017).

Têm sido celebrados memorandos de entendimento (MoU) que melhoram a proficiência do CCD. Em 2016, foi assinado um MoU entre o Estado Português e a OTAN "sobre cooperação em ciberdefesa com vista a promover a troca de informações, incluindo ameaças ciber e partilha de boas práticas" (Defesa Nacional, 2016). Desde o corrente ano, fruto de um MoU entre o CCD e o CNCS, há partilha de informação, obtendo-se assim uma imagem global da ameaça no ciberespaço nacional (Público, 2017).

Atualmente o CCD está equipado com "(…) meios materiais necessários à condução de operações no Ciberespaço (…)", o mesmo acontece com as infraestruturas, cujos investimentos têm vindo a colmatar as limitações. De qualquer modo, a capacidade de condução de operações no ciberespaço, só será viável após avaliação da força em que estará inserido e das capacidades e vulnerabilidades da força adversária (Farinha & Assunção, 2017).

O CCD é uma estrutura pequena conjunta, que conta com 10 militares (Público, 2017), com formação específica e dispendiosa (Vinagreiro, 2017). Mas aqui reside um desafio: os 10 militares são suficientes para as operações diárias, mas a necessidade de alocar recursos humanos (RH) para funções que não tinham sido previstas tornam o atual número reduzido. Para "(…) situações de condução de operações no ciberespaço que requeiram um número maior de elementos, está prevista a integração de *augmentees* provenientes das CIRC dos três ramos, que de forma temporária passam a desempenhar as suas funções no CCD" (Farinha & Assunção, 2017).

Entre os entrevistados das CIRC dos ramos, também há a noção que o número de RH (do CCD e das equipas CIRC dos ramos), não é o suficiente. O Major Valente salientou que "os elementos especializados em ciberdefesa não são suficientes para as operações ofensivas e defensivas necessárias para travar uma ciberguerra" (2017) e o Capitão-tenente Baptista das Neves constatou que a determinação das classes militares para a área, dificulta as próprios CIRC dos ramos (2017), o que foi realçado pelo Major Vinagreiro, em que "(…) o grau de aprendizagem e especificidade técnica, não é compatível com a gestão de pessoal(…)" (2017).

Segundo o Tenente-coronel Paulo J. Branco, Portugal estuda a possibilidade de evoluir para um Comando de Ciberdefesa com uma capacidade maior (Público, 2017), passando de "um centro coordenador e capacidades nos três ramos" para um comando conjunto (Diário de Notícias, 2017), com um incremento de RH e mais funções que as previstas para os 10 militares do CCD, o que poderá ser a solução para o problema do

reduzido número dos RH. Esta solução é partilhada pelos entrevistados das CIRC dos ramos. Contudo, o Capitão-tenente Baptista das Neves defende a centralização de RH (2017), enquanto o Major Valente e o Major Vinagreiro são da opinião que o Comando devia ser reforçado com mais RH e os ramos deviam continuar com as CIRC, devido ao conhecimento local das diferentes redes e sistemas dos ramos e da capacidade de intervenção imediata (Valente, 2017) (Vinagreiro, 2017).

Outra possibilidade seria, mediante as necessárias alterações legais, aproveitar as aptidões de civis (Leite, 2017), com abordagens semelhantes às usadas pela China ou pela Estónia, esta possibilidade teria de ser analisada (Farinha & Assunção, 2017), pois seria uma alteração no modo das FFAA Portuguesas atuarem. Atualmente as operações militares efetuadas pelas FFAA Portuguesas são apenas operadas por militares, com formação e doutrina militar. A abertura para civis poderia desvirtuar o conceito de militar, cujo estatuto é diferente, do mesmo modo que poderia criar oportunidades da ingerência de interesses privados nas operações militares. No caso concreto das operações no ciberespaço, permitiria que o *Know How* existente na população fosse aproveitado para alcançar objetivos nacionais, com custos mais reduzidos, pois eram convocados apenas em necessidade e com custos de formação inexistentes.

Uma solução descartada seria a da junção do CCD e do CNCS, devido às respetivas missões serem diferentes, não havendo assim mais-valia (Farinha & Assunção, 2017) e porque os âmbitos são diferentes, as "(…) entidades tendem a confiar primariamente naquelas com quem mantêm relações de afinidade, quer seja de negócio ou da sua natureza" (Raposo, 2017).

A gestão dos RH é outro desafio, a formação é extensa, requer uma seleção criteriosa e a permanência nas funções deve ser mais longa (Farinha & Assunção, 2017), sendo que este desafio "(…) deveria comprometer os ramos na gestão que faz (…)" (Vinagreiro, 2017).

A instalação da *NATO Communications and Information Systems School* em Portugal é uma janela de oportunidade para a formação e treino e incentiva a criação de uma cultura de cibersegurança em Portugal e que pode potenciar o enfoque das nossas FFAA para a área da ciberdefesa.

Num país com um índice nas novas tecnologias crescente, com limitações orçamentais que não permitem investimento em material de guerra e número reduzido de RH nas FFAA, o investimento em formação de qualidade na área da ciberdefesa

contribuiria para equilibrar o poder militar e aumentar as capacidades nacionais, constituindo-se como uma mais-valia nos compromissos internacionais que Portugal assumiu.

3. Análise

Depois de caraterizar o ciberespaço, enquadrar a ciberguerra e diferenciar a cibersegurança da ciberdefesa, (concretamente a ciberdefesa nacional), é possível responder às PD e assim consolidar a resposta à PP.

PD 1 - Existe presentemente necessidade de dotar Portugal de capacidades para operar em contexto de ciberguerra?

As caraterísticas e particularidades do ciberespaço têm condições excecionais para o aproveitamento de oportunidades. Mas a sua grande exposição evidencia vulnerabilidades, em que os ciberataques têm crescido exponencialmente. As nossas IC estão sob a exigência de comportamentos e medidas de segurança, mas a ameaça é real. Daí terem sido emanadas diretivas pela UE que se consumaram em Portugal através da criação do CNCS.

De qualquer modo, ataques cibernéticos já ocorridos, demonstraram que a fronteira entre a ciberpaz e a ciberguerra é ténue.

A astúcia de alguns atores estatais relativamente ao Direito Internacional e a frágil intervenção das NU ao regulamentar o ciberespaço têm possibilitado que sejam exercidas operações no ciberespaço, com efeitos negativos para os Estados atacados.

Tanto a OTAN como a UE têm-se esforçado para a edificação ou maturação de capacidades de ciberdefesa entre os países membros.

Neste contexto, Portugal deve dotar-se de capacidades para exercer ciberoperações em contexto de ciberguerra, não só para garantir proteção, resiliência e segurança das redes, assegurar a liberdade de ação, mas também contribuir para a cibersegurança nacional e Euro-Atlântica.

PD 2 - O CCD tem os meios necessários para exercer ciberoperações?

O CCD está equipado com as infraestruturas, os meios materiais e RH, incluindo a possibilidade de integração de *augmentees* provenientes das CIRC dos três ramos, necessários para exercer ciberoperações, pese embora qualquer viabilidade de as exercer carece de avaliação das capacidades da força em que está inserida e das vulnerabilidades

da força dos adversários, o que pode vir a revelar necessidade de mais meios materiais e onde os RH podem vir a demonstrar-se escassos.

PD 3 - Existem capacidades que merecem ser melhoradas para dotar o CCD de uma capacidade relevante para operar no contexto internacional?

O CCD constitui-se como um órgão recente, em que a edificação da capacidade e os MoU estabelecidos contribuem para uma melhor capacidade ao nível internacional, mas há desafios que têm de ser considerados de modo a robustecer as atuais capacidades. A evolução para um cibercomando conjunto com atribuições semelhantes à abordagem dos EUA, poderia debelar alguns constrangimentos, nomeadamente o número reduzido de RH. Por outro lado, deve ser dado ênfase à edificação de uma doutrina conjunta e uma organização que a suporte, assim como à gestão dos RH, concretamente ao recrutamento, formação, treino e permanência nas funções.

Deste modo é possível induzir uma teoria, que se fundamenta em análise de dados particulares que consubstanciam a resposta à PP.

PP - A atual estrutura definida para a ciberdefesa nacional tem a capacidade para exercer ciberoperações no contexto internacional?

Atualmente, a estrutura definida para a ciberdefesa nacional tem a capacidade para exercer ciberoperações no contexto internacional, mas deverão ser empregues esforços para robustecer essa estrutura, ao nível da doutrina e RH.

Conclusões e Recomendações

Este trabalho de investigação pretendeu avaliar a atual capacidade da estrutura definida para a ciberdefesa nacional, permitindo assim aferir as suas valências e as vulnerabilidades no contexto internacional, mais concretamente no caso de haver necessidade de exercer operações no ciberespaço no contexto internacional, ultrapassando a fronteira entre o que é a ciberpaz e a ciberguerra. Isto porque é cada vez mais premente para os Estados munirem-se de meios de controlo no âmbito da cibersegurança e da ciberdefesa.

Para a correta avaliação foram consideradas as ameaças, os ataques conhecidos, as capacidades internacionais, o pessoal efetivo e qualificado existente e os equipamentos disponíveis.

O grande enfoque da avaliação efetuada foi nas capacidades atuais da ciberdefesa nacional, com especial atenção no CCD.

O percurso metodológico seguido está conforme à NEP/ACA – 010 (IESM, 2015b), tendo a investigação sido desenvolvida segundo um raciocínio indutivo, assente numa estratégia de investigação qualitativa, através de um estudo de caso, fundamentado em análise documental e entrevistas semiestruturadas.

A escolha desta metodologia tem a ver com a necessidade de recolher dados descritivos, que não se traduzem em números, sobre um contexto específico, a ciberdefesa nacional, provenientes de livros, documentos, trabalhos e noticias consultadas e também das entrevistas elaboradas, que permitem de particularidades estabelecer generalizações.

As principais linhas consubstanciaram-se num percurso metodológico assente em três fases: a fase exploratória, fase analítica e a fase conclusiva.

Na fase exploratória, houve a necessidade de efetuar entrevistas exploratórias e leituras preliminares, para assim haver um correto enquadramento do tema, a contextualização do panorama atual e a criação de uma base concetual. Ainda nesta fase foi possível delimitar o objeto da investigação, e a definição dos objetivos geral e específicos da mesma. Do problema da investigação surgiram as perguntas de partida e derivadas.

Na fase analítica, foram recolhidos os dados através de análise documental e entrevistas semiestruturadas. Posteriormente foram analisados os dados antes recolhidos, com grande enfoque na análise documental e cujas entrevistas passaram por transcrição,

leitura, construção de sinopses e análises descritiva e interpretativa. No fim, foram apresentados os dados, através de descrições estruturadas por capítulos e subcapítulos e algumas figuras e tabelas.

Na fase conclusiva, foi efetuada a avaliação, interpretação e discussão dos dados obtidos de modo a dar resposta às PD. Posteriormente, são apresentadas as conclusões e respetivas recomendações.

3.1. **Avaliação dos Resultados**

Assim, considera-se que foi respondida a PP deste trabalho: A atual estrutura definida para a ciberdefesa nacional tem capacidade para exercer ciberoperações no contexto internacional?

Como corpo de resposta à PP, foram satisfeitas as PD:

PD 1 - Existe presentemente necessidade de dotar Portugal de capacidades para operar em contexto de ciberguerra?

PD 2 - O CCD tem os meios necessários para exercer ciberoperações?

PD 3 - Existem capacidades que merecem ser melhoradas para dotar o CCD de uma capacidade relevante para operar no contexto internacional?

Foram também alcançados os objetivos, concretamente:

O objetivo geral:

- Avaliar as capacidades da atual estrutura definida para a ciberdefesa nacional.

Os objetivos específicos:

- Identificar a fronteira entre a ciberpaz e a ciberguerra;
- Identificar os meios de que Portugal dispõe, na área da defesa, para exercer operações no ciberespaço;
- Identificar os aspetos a desenvolver na ciberdefesa nacional;
- Propor recomendações para melhorar a atual capacidade da ciberdefesa nacional.

Foi então possível apurar que a atual estrutura definida para a ciberdefesa nacional tem a capacidade para exercer ciberoperações no contexto internacional, pois está equipada com infraestruturas e meios materiais necessários para exercer ciberoperações, pese embora a necessidade de avaliar a viabilidade de as exercer face às capacidades da força em que está inserida e das vulnerabilidades da força adversária. Os RH existentes, com a possibilidade de reforço com *augmentees*, têm a capacidade para executar operações. De

qualquer modo, os RH podem vir a revelar-se escassos, devido às múltiplas tarefas que têm de desenvolver que não tinham sido previstas aquando da edificação da capacidade. Deste modo, ficou apurado que deverão ser empregues esforços para robustecer essa estrutura de modo a não comprometer os compromissos assumidos.

Foi também identificado que a fronteira entre a ciberpaz e a ciberguerra é ténue, embora a doutrina tenha vindo a clarificar os critérios de distinção. Tem sido defendido por vários especialistas que a Lei Internacional se aplica às operações cibernéticas, em particular, a decisão judicial sobre o caso da Nicarágua, que esclarece que há ações que constituem uso da força sem constituir um ataque armado. Ainda neste contexto, houve a necessidade de abordar os acontecimentos da Estónia, Geórgia e o caso do vírus "Stuxnet", em que o critério de Schmitt foi considerado para decidir se os acontecimentos compreendiam os requisitos de um ataque armado.

Foram identificados e descritos os vários tipos de operações no ciberespaço assim como as ações que as materializam.

Foi também constatado que os MoU estabelecidos pelo CCD contribuem para uma melhor capacidade ao nível nacional e internacional, mas há desafios que têm de ser considerados de modo a robustecer as atuais capacidades. A evolução para um cibercomando, ou uma abordagem que aproveite as aptidões de civis, pode vir a debelar alguns constrangimentos atuais, (essencialmente ao nível da gestão dos RH), devendo ser dado enfâse à edificação de uma doutrina conjunta e uma organização que a suporte.

3.2. **Contribuições**

Este trabalho contribui para um melhor entendimento da ameaça cibernética e de como Portugal se tem esforçado para implementar medidas que aumentem a sua resiliência.

Esta ameaça existe devido ao ciberespaço, que é um espaço digital, formado por componentes físicos e não físicos, *hardware* e *software*, mas também por pessoas que interagem ao nível do armazenamento, modificação e troca de dados e ao nível da interação social. É um espaço com caraterísticas e particularidades com condições excecionais para o aproveitamento de oportunidades.

O trabalho contribui assim para um melhor entendimento do que é o ciberespaço e quais as suas especificidades, mas alerta que é um espaço que tem permitido que diversos atores usufruam conflitualmente dele, tornando-se ameaças. As IC dos Estados encontram-

se como potenciais alvos destas ameaças, posicionando-se como vulnerabilidades – ficando vulneráveis a ciberataques.

Este trabalho permite esclarecer a origem do CNCS, como consumação de uma estratégia nacional, que foi a repercussão de diretivas emanadas pela UE face à afirmação das ameaças, constatadas pelo aumento de incidentes, com a intenção de criar uma cultura de cibersegurança.

Houve também o contributo para esclarecer as questões jurídicas que têm sido alvo de investigação e criação de doutrina nas matérias relacionados com conflitos cibernéticos.

Foram identificados estudos que contribuem para uma ideia do atual poder cibernético mundial e para confirmar a ideia que as matérias relativas à ciberdefesa estão em carteira nas grandes potências mundiais, mas também em países que vêm nestas capacidades uma possibilidade criar poder dissuasor e equilibrar o poder

Foi também constatado que tanto a OTAN como a UE têm-se esforçado para a edificação ou maturação de capacidades de ciberdefesa entre os países membros, onde foram identificados momentos cruciais nas políticas das organizações, contribuindo assim para um melhor entendimento da origem de decisões tomadas.

Foi também explicada a astúcia de alguns atores estatais relativamente ao Direito Internacional e a frágil intervenção das NU ao regulamentar o ciberespaço, que tem possibilitado que sejam exercidas operações no ciberespaço, com efeitos negativos para os Estados atacados. Esta situação contribui para um melhor entendimento sobre algumas decisões políticas, militares, jurídicas e permite saber que tem havido iniciativas, como a da "Microsoft", com o intuito da criação de tratados internacionais sobre o ciberespaço, de modo a proteger os interesses de quem utiliza o ciberespaço. Face a estas adversidades, fica a ideia que as organizações internacionais armem sinergias e criem algo como as "Nações Unidas Digitais", e tornem possível vislumbrar no futuro, forças de "capacetes azuis virtuais" capazes agir em caso de ciberataques.

3.3. **Recomendações**

Fruto da investigação foi possível apurar as dificuldades que a capacidade de ciberdefesa nacional enfrenta relativamente ao nível dos RH.

É recomendável que haja um comprometimento dos ramos das FFAA na gestão dos RH para a área da ciberdefesa, onde o cabimento de RH seja aumentado, o recrutamento

seja criterioso e o tempo de permanência nas funções seja longo, em suma uma carreira na área da ciberdefesa.

De modo a melhorar a interoperabilidade entre os RH da área da ciberdefesa, deve ser edificada uma doutrina conjunta e uma organização que a suporte, assim como a continuidade dos exercícios conjuntos.

A evolução para um cibercomando ou outra abordagem similar pode contribuir para um incremento de RH e mais funções que as previstas para os 10 militares do CCD, debelando os constrangimentos de RH. Mas devido à diferença das redes e sistemas dos ramos, as equipas CIRC dos ramos devem continuar a existir, pois têm o conhecimento local a capacidade de intervenção imediata.

O investimento em ciberdefesa é consideravelmente mais baixo que em outras áreas militares e as contrapartidas são vantajosas. Os atores menos poderosos têm incentivado o investimento nesta área de modo a equilibrar o poder. Portugal deveria ter este assunto em consideração.

A instalação da *NATO Communications and Information Systems School* em Portugal cria uma janela de oportunidade para a formação e treino, que incentiva a criação de uma cultura de cibersegurança em Portugal.

3.4. **Limitações**

A capacidade de ciberdefesa nacional é muito recente, pelo que a procura de informação é restrita e há informação que não se encontra disponível para o público em geral. Há também limitações ao nível do espaço físico de procura nacional, refletido neste trabalho com a restrita escolha de áreas, concretamente ao CCD, às CIRC dos ramos e ao CNCS, de onde são provenientes os entrevistados.

Ao nível internacional há muita informação, o que prejudica a delimitação da procura, mas ao mesmo tempo há pouco informação específica, porque os Estados não pretendem que certa informação seja do conhecimento público.

De qualquer modo, estas limitações deixam em aberto outras pesquisas, nomeadamente:

- Estudo sobre a evolução para um cibercomando;
- Estudo sobre diferentes abordagens para a evolução do CCD;
- Estudo sobre a gestão de RH para funções de ciberdefesa;
- Estudo sobre a edificação de doutrina conjunta;
- Estudo sobre a interoperabilidade entre o CCD e a CIRC dos ramos;

- Estudo sobre a interoperabilidade entre o CCS e o CNCS;
- Estudo sobre o impacto financeiro entre a investimento versus contrapartidas das várias capacidades militares.

Bibliografia

ABI Research, 2015. *Global Cybersecurity Index & Cyberwellness Profiles.* Genebra: ITU.

Anon., 2016. *U.S. Strategic Command.* [Em linha] Disponível em: http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ [Acedido em 15 mai. 2017].

ANPC, 2016. *Infraestruturas críticas.* [Em linha] Disponível em: http://www.prociv.pt/pt-pt/RISCOSPREV/INFRAESTRUTURASCRITICAS/Paginas/default.aspx [Acedido em 09 dez. 2016].

AR, 2005. *Constituição da República Portuguesa Sétima Revisão Constitucional – 2005.* Lisboa: Assembleia da República.

Aslanoglu, R. & Tekir, S., 2012. *Proceedings of the 11th European Conference on Information warfare and security.* Laval, Eric Filiol and Robert Erra.

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

CCDCOE, 2009. *Manual de Tallinn.* 1ª ed. Tallinn: Cambridge University Press.

CCDCOE, 2015. *About Cyber Defence Centre.* [Em linha] Disponível em: https://ccdcoe.org/about-us.html [Acedido em 08 dez. 2016].

CCDCOE, 2015. *United Nations Group of Governmental Experts Achieve a 'Landmark Consensus'.* [Em linha] Disponível em: https://ccdcoe.org/united-nations-group-governmental-experts-achieve-landmark-consensus.html [Acedido em 23 abr. 2017].

CCDCOE, 2016. *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit.* [Em linha] Disponível em: https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html [Acedido em 28 jan. 2017].

CCDCOE, 2017. *Professor Michael N. Schmitt.* [Em linha] Disponível em: https://ccdcoe.org/cyberwarfare/439.html [Acedido em 27 abr. 2017].

Clark, D., 2010. *Characterizing cyberspace: past, present and future,* Massachusetts: ECIR Working Paper.

Clarke, R. A. & Knake, R. K., 2010. *Cyber War The Next Threat to National Security and What to Do About It.* New York: Harpercollins Publishers Inc.

CNCS, 2016a. *CERT.PT.* [Em linha] Disponível em: https://www.cncs.gov.pt/certpt/ [Acedido em 07 jan. 2017].

CNCS, 2016b. *Membros da rede nacional de CSIRT.* [Em linha] Disponível em: http://www.cert.rcts.pt/index.php/rede-nacional-csirt/directorio [Acedido em 12 abr. 2017].

Comissão Europeia, 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Bruxelas: High Representative of the European Union for Foreign Affairs and Security Policy.

CUE, 2008. *Directiva 2008/114/CE do Conselho.* Bruxelas: Jornal Oficial da União Europeia.

CUE, 2016. *Directiva 2016/1148 do Parlamento Europeu e do Conselho.* Bruxelas: Jornal Oficial da União Europeia.

Daily Mail, 2010. *Computer super-virus 'targeted Iranian nuclear power station' but who made it?.* [Em linha] Disponível em: http://www.dailymail.co.uk/sciencetech/article-1314580/Stuxnet-worm-targeted-Iranian-nuclear-power-station-sophisticated-virus-attack-ever.html [Acedido em 10 mar. 2016].

Defesa Nacional, 2016. *Portugal e NATO reforçam cooperação em Ciberdefesa.* [Em linha] Disponível em: http://www.defesa.pt/Paginas/PortugaleNATOrefor%C3%A7amcoopera%C3%A7%C3%A3oemCiberdefesa.aspx [Acedido em 05 jun. 2017].

De, K., 2016. *Peek into Tallinn Manual - Analyzing Estonia, Georgia & Stuxnet Cyber Attacks against this background.* [Em linha] Disponível em: https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/01/14/peek-tallinn-

manual-analyzing-estonia-georgia-stuxnet-cyber-attacks-against
[Acedido em 24 abr. 2017].

Diário de Notícias, 2017. *Comando para ciberdefesa em estudo mas sem prazos para decisão - subdiretor-geral de Defesa.* [Em linha] Disponível em: http://www.dn.pt/lusa/interior/comando-para-ciberdefesa-em-estudo-mas-sem-prazos-para-decisao---subdiretor-geral-de-defesa-8500291.html
[Acedido em 22 jun. 2017].

Dicionário Priberam da Língua Portuguesa, 2008a. *ciberameaça.* [Em linha] Disponível em: http://www.priberam.pt/dlpo/ciberamea%C3%A7a
[Acedido em 09 dez. 2016].

Economist Intelligence Unit, 2011. *Cyber Power Index: Findings and Methodology.* EUA: Booz Allen Hamilton Inc.

Economist Intelligence Unit, 2017. *Economist Intelligence Unit.* [Em linha] Disponível em: http://www.eiu.com/home.aspx
[Acedido em 15 mai. 2017].

ENISA, 2015. *ICS SCADA.* [Em linha] Disponível em: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada
[Acedido em 07 jan. 2017].

Expresso, 2017. *Os capacetes azuis das ciberguerras.* [Em linha] Disponível em: http://expresso.sapo.pt/sociedade/2017-03-19-Os-capacetes-azuis-das-ciberguerras
[Acedido em 13 abr. 2017].

FA, 2011. RFA 390-6. Em: DIVCSI, ed. *POLÍTICA DE CIBERDEFESA DA FORÇA AÉREA.* Alfragide: Força Aérea, p. 3.

Farinha & Assunção, 2017. *Entrevista ao CCD* [Entrevista] (15 Março 2017).

Fernandes, J. P. T., 2014. *Ciberguerra Quando a Utopia se Transforma em Realidade.* Lisboa: Verso da História.

FM3-38, 2014. *Cyber Electromagnetic Activities.* EUA: Headquarters, Department of the Army.

Gallis, P., 2008. *The NATO Summit at Bucharest, 2008,* Washington, D.C.: Congressional Researh Service.

Ghernaouti, S., 2013. *Cyber Power: Crime, Conflict and Security in Cyberspace.* Lausanne: EPFL Press.

Global Risk Advisors, 2016. *The United Nations and Cyberwarfare.* [Em linha] Disponível em: https://globalriskadvisors.com/blog/united-nations-cyber-warfare/ [Acedido em 05 jun. 2017].

Grauman, B., 2012. *Cyber-security: The vexed question of global rules.* Bruxelas: Security & Defence Agenda.

Grossman-Vermaas, R., 2004. *Discourse of action: Command, Control, Conflict and the Effects Based Approach,* Canadá: National Defence Headquarters, Directorate of Defence Analysis.

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

IESM, 2014. *Orientações metodológicas para a elaboração de trabalhos de investigação*. Lisboa: IESM.

IESM, 2015a. *Regras de Apresentação e Referenciação para os Trabalhos Escritos a realizar no IESM - NEP / ACA 018.* Lisboa: IESM.

IESM, 2015b. *Trabalhos de Investigação - NEP / ACA - 10.* Lisboa: IESM.

Inductive Automation, 2016. *What is SCADA?.* [Em linha] Disponível em: https://inductiveautomation.com/what-is-scada [Acedido em 21 jun. 2017].

International Court of Justice, 1986. *Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).* The Hague: s.n.

ITU, 2017. *About International Telecommunication Union (ITU).* [Em linha] Disponível em: https://www.itu.int/en/about/Pages/default.aspx [Acedido em 15 mai. 2017].

IUM, 2016. *Orientações metodológicas para a elaboração de trabalhos de investigação.* Lisboa: IUM.

Joint Publication 3-12 (R), 2013. *Cyberspace Operations.* EUA: Join Chiefs of Staff.

Klimburg, A., 2012. *National Cyber Security Framework Manual.* Tallinn: NATO CCD COE Publication.

Langner, R., 2012. *Cyber Warfare* , Hamburgo: Langner Communications.

Leite, 2017. *Entrevista ao Coordenador Jurídico do CNCS* [Entrevista] (24 Março 2017).

Marinha, 2016. Revista da Armada. *Cibersegurança e ciberdefesa − Portugal e NATO*, Maio, pp. 4-5.

McAfee, 2012. *57% Believe a Cyber Arms Race is Currently Taking Place, Reveals McAfee-Sponsored Cyber Defense Report.* [Em linha] Disponível em: https://www.mcafee.com/sg/about/news/2012/q1/20120130-02.aspx [Acedido em 15 mai. 2017].

MDN, 2011. *Decreto-Lei n.º 62/2011*. Lisboa: Diário da República.

MDN, 2013. *Diretiva Iniciadora com Orientação Política para a Ciberdefesa.* Lisboa: Diário da República.

MDN, 2014. *Decreto-lei 184/2014.* Lisboa: Diário da República.

MDN, 2015. *Decreto Regulamentar n.º 13/2015.* Lisboa: Diário da República.

Ministro da Defesa Nacional, 2016. *Portugal na Vanguarda da Formação para a Ciberdefesa.* [Em linha] Disponível em: http://www.portugal.gov.pt/pt/ministerios/mdn/noticias/20160428-mdn-ciberdefesa.aspx [Acedido em 05 jun. 2017].

NCIA, 2012. *Connecting Forces.* [Em linha] Disponível em: https://www.ncia.nato.int/About/Pages/About-the-NCI-Agency.aspx [Acedido em 08 dez. 2016].

NCIA, 2017. *Cyber Security.* [Em linha] Disponível em: https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx [Acedido em 05 jun. 2017].

Neves, B. d., 2017. *Entrevista à CIRC da Marinha* [Entrevista] (15 Maio 2017).

Nextgov, 2016. *These Perks Could Entice Hackers to Work for CYBERCOM. But does HR Know About Them?.* [Em linha] Disponível em: http://www.nextgov.com/cybersecurity/2016/02/congress-member-says-cybercom-hr-needs-schooling-legal-pay-packages/125997/ [Acedido em 05 jun. 2017].

NU, 1945. *Charter of the United Nations and Statute of the International Court of Justice.* San Francisco: s.n.

NU, 2013. *The Cyber Index.* Geneva: UNIDIR.

Nunes, P. V., 2016. *Sociedade em Rede, Ciberespaço e Guerra de Informação.* 2ª ed. Lisboa: Instituto de Defesa Nacional.

Nunes, P. V., 2017. *Ciberdefesa: O Desafio do Século XXI.* Lisboa, Assembleia da República.

OTAN, 2008. *Bucharest Summit Declaration.* [Em linha] Disponível em: http://www.nato.int/cps/in/natohq/official_texts_8443.htm [Acedido em 05 jun. 2017].

OTAN, 2010. *Strategic Concept.* Lisboa: NATO Public Diplomacy Division.

OTAN, 2017a. *Cyber defence.* [Em linha] Disponível em: http://www.nato.int/cps/en/natohq/topics_78170.htm [Acedido em 05 jun. 2017].

OTAN, 2017b. *Cyber Defence: Home.* [Em linha] Disponível em: http://www.natolibguides.info/cybersecurity [Acedido em 05 jun. 2017].

Palma, M. F., 2012. *Conceito material de crime, direitos fundamentais e reforma penal.* [Em linha] Disponível em: http://www.fd.unl.pt/docentes_docs/ma/TQB_MA_22910.pdf [Acedido em 22 jun. 2017].

Parlamento Europeu, 2014. *Cyber defence in the EU.* Bruxelas: European Parliamentary Research Service.

PCguia, 2016. *Marsh divulga resultados do 'Continental European Cyber Risk Survey: 2016 Report'.* [Em linha] Disponível em: http://www.pcguia.pt/2016/11/marsh-divulga-resultados-do-continental-european-cyber-risk-survey-2016-report/ [Acedido em 06 jan. 2017].

PCM , 2014. *Decreto-Lei n.º 69/2014.* Lisboa: Diário da República.

PCM, 2013. *Resolução do Conselho de Ministros n.º 26/2013.* Lisboa: Diário da República.

PCWorld, 2012. *When Is a Cybercrime an Act of Cyberwar?.* [Em linha] Disponível em: http://www.pcworld.com/article/250308/when_is_a_cybercrime_an_act_of_cyberwar_.html [Acedido em 15 abr. 2017].

Público, 2017. *Dez militares "combatem" online há dois anos para proteger redes das Forças Armadas.* [Em linha]

Disponível em: https://www.publico.pt/2017/05/22/tecnologia/noticia/dez-militares-combatem-ha-dois-anos-no-ciberespaco-para-proteger-redes-das-forcas-armadas-1773006

[Acedido em 22 mai. 2017].

Quivy, R., 2005. *Manual de Investigação em Ciências Sociais. 4 ed.*. Lisboa: Gradiva.

Ralo, J., 2013. *Artigo de Opinião- Cibersegurança e Ciberdefesa.* [Em linha] Disponível em: http://dgpdn.blogspot.pt/2013/03/artigo-de-opiniao-ciberseguranca-e.html

[Acedido em 21 jun. 2017].

Raposo, 2017. *Entrevista ao Consultor Coordenador do Departamento de Operações do CNCS* [Entrevista] (24 Março 2017).

Santos, J. L. d., 2014. *O Futuro da Guerra.* Lisboa: Nova Vega.

Schmitt, M. N., 1999. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law,* Volume 37, pp. 885-937.

Schmitt, M. N., 2012. *The 'Use of Force' in Cyberspace: A Reply to Dr Ziolkowsk.* Tallinn, NATO CCD COE Publications.

Silva, N. M. d., 2016. *Cooperação OTAN - UE,* Lisboa: FCSH.

The New York Times, 2008. *Before the Gunfire, Cyberattacks.* [Em linha] Disponível em: http://www.nytimes.com/2008/08/13/technology/13cyber.html [Acedido em 09 dez. 2016].

The Washington Times, 2016. *PLA on cyberwarfare buildup.* [Em linha] Disponível em: http://www.washingtontimes.com/news/2016/feb/17/inside-the-ring-china-plans-cyberwarfare-force-to-/

[Acedido em 12 jun. 2017].

theguardian, 2007. *Russia accused of unleashing cyberwar to disable Estonia.* [Em linha] Disponível em: https://www.theguardian.com/world/2007/may/17/topstories3.russia [Acedido em 09 dez. 2016].

United States Department of Defense, 2016. *Defense Budget Overview.* EUA: Department of Defense.

USAWC, 2016. *Strategic Cyberspace Operations Guide.* EUA: Center for Strategic Leadership.

Valente, 2017. *Entrevista à CIRC da Força Aérea* [Entrevista] (15 Maio 2017).

Vinagreiro, 2017. *Entrevista à CIRC do Exército* [Entrevista] (09 Junho 2017).

World Economic Forum, 2016. *What you need to know about the G20.* [Em linha] Disponível em: https://www.weforum.org/agenda/2016/09/what-you-need-to-know-about-the-g20/
[Acedido em 15 mai. 2017].

Ziolkowski, K., 2012. *Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-Criteria" for Use of Force.* Tallinn, NATO CCD COE Publications.

Apêndice A - Modelo Conceptual

Tabela 2 - Modelo Conceptual

Pergunta de partida	Perguntas derivadas	Conceitos	Dimensões	Instrumentos de Observação
PP: A atual estrutura definida para a ciberdefesa nacional, tem capacidade para exercer ciberoperações no contexto internacional?	**PD1:** Existe presentemente necessidade de dotar Portugal de capacidades para operar em contexto de ciberguerra?	Ciberespaço Infraestruturas críticas Ciberameaça Ciberoperações Ciberguerra Ciberdefesa	Jurídica	Análise Documental
			Política	
			Operacional	Análise Documental Entrevistas
			Relações Internacionais	
	PD2: O CCD tem as ferramentas/meios necessários para exercer ciberoperações?	Ciberoperações Ciberdefesa Cibersegurança	Política	Análise Documental
			Recursos Humanos	Análise Documental Entrevistas
			Logística	
	PD3: Existem capacidades que merecem ser melhoradas para dotar o CCD de uma capacidade relevante para operar no contexto internacional?	Ciberdefesa	Jurídica	Análise Documental
			Política	
			Económica	
			Relações Internacionais	Análise Documental Entrevistas
			Recursos Humanos	
			Logística	
			Virtual	

Apêndice B - Ciberespaço

Caraterísticas

Segundo David Clark (2010) estas caraterísticas agrupam-se em quatro camadas:

- A camada física, onde no espaço geográfico/físico se enquadram todos os dispositivos físicos (*hardware*) onde o ciberespaço existe, concretamente os computadores, servidores, sensores, redes de computadores e canais de comunicação (Clark, 2010).
- A camada lógica, onde os sistemas de informação se enquadram, onde se encontram os componentes que disponibilizam serviços (essencialmente na internet) e que residem na camada física. David Clark (2010) afirma que a força e as limitações do ciberespaço são maioritariamente consequência das decisões tomadas ao nível desta camada.
- A camada da informação, onde toda a informação criada, capturada, armazenada e processada existe. Desde vídeos, músicas, livros, imagens, registos escritos, as próprias páginas da internet, meta-informação e até mesmo a informação referente ao histórico de interações (Clark, 2010).
- A camada referente às pessoas (social), a camada mais importante, onde se enquadram os cibernautas. A importância desta camada é enfatizada por David Clark (2010), pois considera que são as pessoas que moldam o seu personagem no ciberespaço e as suas ações é que justificam a existência das grandes plataformas de sistemas de informação, como exemplo refere que o Wikipédia só existe porque há o contributo das pessoas e o Twitter existe porque as pessoas interagem através dele.

Segundo FM3-38 (2014) e *United States Army War College* (USAWC) (2016), o ciberespaço está dividido em 3 camadas, as camadas física, lógica e referente às pessoas (social). Esta visão não difere muito da ideia defendida por David Clark (2010), mas tem a particularidade de integrar a camada da informação na camada lógica, que é justificada em FM3-38 (2014) por a camada lógica ser uma abstração da camada física e onde a informação é gerada, armazenada e processada pelos sistemas de informação, sistemas estes que também residem na mesma camada.

Particularidades

É nestas camadas que as valências do ciberespaço se evidenciam, proporcionando grandes mais-valias na era da globalização, pois, segundo USAWC (2016, p. 6), através do ciberespaço, as trocas de informações são rápidas (por vezes instantâneas) e dinâmicas, melhorando por exemplo as transações financeiras assim como as trocas e o rastreio de mercadorias e produtos. Ainda na referida publicação estão descritas particularidades do ciberespaço

- Pode ter a capacidade de engenharia reversa, que pressupõe o reuso do código utilizado em operações no ciberespaço e que possibilita o efeito contrário, (uso do mesmo código contra o seu criador);
- Não é propriedade nacional ou internacional, pois permite o fluxo livre de informação, onde a clareza das fronteiras territoriais é pouca.
- Falta de cooperação ou colaboração internacional, essencialmente a nível jurídico e regulamentar, que dificulta o rastreio da origem de uma operação e assim ludibriar a confiança em organizações.
- Baixo custo, quer em componentes físicos, código e até mesmo em formação na área, comparativamente até mesmo noutras vertentes militares, mais concretamente o custo de aquisição, manutenção e formação em áreas como os navios, aeronaves e mísseis.
- Volátil, o ciberespaço como materialização das comunicações e sistemas de informação sofre do mal representado na expressão “o que hoje é, amanhã é passado”, pois quando é alcançada uma vantagem e identificada uma vulnerabilidade no opositor, esta tende a ser de curta duração, rapidamente o opositor debela essa vulnerabilidade e deixa de existir essa vantagem.
- Rápida, concretamente na execução de operações, no entanto pode ser lenta na preparação dessas mesmas operações.
- Efeitos em cascata não intencionais, pois no ciberespaço não é fácil prever o comportamento de uma operação e muito menos o alcance da mesma.

Apêndice C - Ameaças

O USAWC (2016) refere a importância que ameaças cibernéticas têm nas estratégias de ataque de diversos atores, considerando que a ciberameaça representa maior perigosidade que a ameaça comum decorrente de atos de terrorismo.

Segundo o USAWC (2016), as ameaças cibernéticas caracterizam-se pelos seguintes aspetos:

- O grande investimento que potenciais adversários têm realizado no ciberespaço, concretamente a Rússia e a China, mas também onde Estados como o Irão e a Coreia do Norte têm investido, potenciando o poder militar, aproveitando o baixo custo relativamente a outras vertentes de cariz ofensivo, como ilustrado na Figura 4.

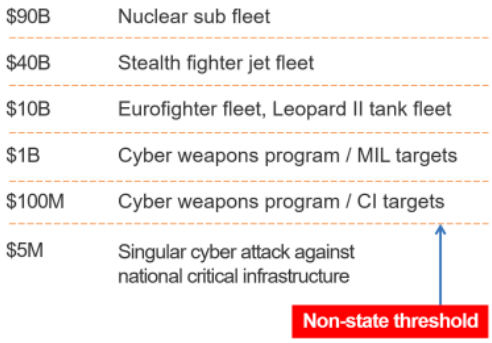

Figura 4 - Economia Militar

Fonte: (Langner, 2012)

- A diversidade de atores, especificados também em Joint Publication 3-12 (R) (2013):
  - Ameaça dos Estados-nação, como a ameaça mais perigosa, devido à facilidade destes atores relativamente a outros em se apetrecharem de recursos físicos e humanos em menor espaço de tempo.
  - Ameaça de atores transnacionais, que estão identificados como organizações que não estão ligados a estados e que têm como forma de alcançar os objetivos o uso do "(…) ciberespaço para angariar fundos, comunicar com públicos-alvo entre si, recrutar, planear operações, desestabilizar a confiança nos governos e conduzir ações terroristas diretas no ciberespaço (…)[11] (Joint Publication 3-12 (R), 2013, pp. I-7)".
  - Ameaça do crime organizado, através de organizações criminosas estatais ou transnacionais que roubam informações através do ciberespaço para bem próprio, para terceiros (efetuando operações de espionagem para atores estatais ou transnacionais) ou para vender.
  - Ameaça de atores individuais ou grupos pequenos que tentam descobrir vulnerabilidades no ciberespaço e que por vezes partilham as descobertas com os proprietários dos sistemas vulneráveis, mas que outras vezes são movidos por outro tipo de motivações menos dignas, quer pessoais quer a sob ordem de organizações.

  E ainda os atores referidos pelo USAWC (2016).
  - Ameaça interna, caraterizada por "(…) um indivíduo que correntemente ou uma vez teve autorização para aceder ao sistema de informações de uma organização, dados ou rede (…)"[11] e que usa da confiança nele depositada para prejudicar a organização ou para proveito próprio.
  - Ameaça natural, mais concretamente através de "(…) inundações, furacões, explosões solares, relâmpagos e tornados (…)"[11], que danificam ou prejudicam o uso do ciberespaço e "(…) oferecem aos adversários a oportunidade de investir sobre a degradação de infraestruturas e desvio de atenção e recursos"[11].
  - Ameaça física, que deve ser antecipada pois é descrita por ser uma ameaça imprevisível no tempo, espaço e no ato em si, por exemplo em que uma "(…) retroescavadora que corta um cabo de fibra ótica de um nó chave do ciberespaço pode interromper a operacionalização do ciberespaço (…)"[11].

Das várias ameaças descritas, é percetível a ideia que os ciberataques são na sua essência ataques deliberados. Deste modo e quanto à origem, podemos considerar os seguintes grupos de ciberameaças (IDN-CESEDEN, 2013):

- "Cibercrime, centradas essencialmente na obtenção de benefícios económicos através de ações ilegais (…)" (IDN-CESEDEN, 2013, p. 22).
- "Ciberespionagem, com foco na obtenção de informações, seja para benefício próprio ou para deter um benefício monetário posterior com a sua venda (…)" (IDN-CESEDEN, 2013, p. 23).
- "Ciberterrorismo, onde se procura um impacto social e político significativo pela destruição física (…)" (IDN-CESEDEN, 2013, p. 23).
- "Ciberguerra, pode ser definida como uma luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha (…)" (IDN-CESEDEN, 2013, p. 23).
- *Hacktivismo* (ciberactivismo), "(…) pelo seu impacto crescente também tem vindo a assumir-se como um campo de ação da ciberameaça (…)" (IDN-CESEDEN, 2013, p. 23).

[11] Tradução do autor.

Apêndice D - Operações no Ciberespaço

Operações no ciberespaço, segundo Joint Publication 3-12 (R) (2013, pp. I-1):

- *Offensive Cyberspace Operations* (OCO) - operações ofensivas, que devem ser autorizadas superiormente através de uma ordem de execução, "(…) destinadas a projetar poder pela aplicação da força no e através do ciberespaço (…)"[12] (Joint Publication 3-12 (R), 2013, pp. II-2), são conduzidas como operações militares numa área de operações, que podem produzir efeitos letais ou não letais em massa, requerem coordenação e integração e são desenhadas para suportar os objetivos e intenções do comandante das forças (FM3-38, 2014, pp. 3-2 e 3-3).
- *Defensive Cyberspace Operations* (DCO) - "(…) são operações passivas e ativas do ciberespaço destinadas a preservar a valência de utilizar capacidades amigáveis do ciberespaço e proteger dados, redes, capacidades centradas na rede e outros sistemas (…)"[12], respondem a atividades não autorizadas ou alertas/informações de ameaças internas e externas do ciberespaço, de modo a restabelecer, voltar a preservar, redirecionar, reconstituir ou isolar redes locais degradadas ou comprometidas (Joint Publication 3-12 (R), 2013, pp. II-2), são conduzidas em "(…)toda a gama de operações militares detetando, identificando e respondendo a inimigos e adversários que tomam ou estão prestes a tomar ações ofensivas contra redes amigas e informações residentes nessas redes(…)"[12] (FM3-38, 2014, pp. 3-6).
  - Medidas de defesa interna, que incluem procura ativa de atividades não autorizadas ou ameaças internas avançadas, bem como as respostas internas a essas situações (Joint Publication 3-12 (R), 2013, pp. II-3).
  - Ações de resposta, que são operações defensivas, que devem ser autorizadas superiormente considerando todas as regras de empenhamento e constrangimentos políticos, que são executadas externamente e pretendem eliminar o ataque ou ameaças que esteja a ser alvo, de modo a defender as capacidades internas do ciberespaço ou outros sistemas, normalmente são executadas ações de contramedidas que degradam as ações atacantes que estejam a ser alvo mas podem não ser suficientes devido a não eliminarem essas mesmas ações atacantes (Joint Publication 3-12 (R), 2013, pp. II-3).
- *Information Network Operations* (INO) - "(…) são ações tomadas para projetar, construir, configurar, proteger, operar, manter e sustentar sistemas e redes de comunicação (…)" internas "(…) de uma forma que crie e preserve a disponibilidade de dados, a integridade, a confidencialidade, bem como autenticação de utilizadores/entidades (…)"[12] (Joint Publication 3-12 (R), 2013, pp. II-3). Segundo o Departamento do Exército dos EUA (2014, pp. 3-7), este tipo de operações passa por:
  - Sistemas integrados, que são infraestruturas internas, seguras e ligadas em rede com redundância e sistemas internos que fornecem informações oportunas e precisas em qualquer ambiente para suportar forças operacionais (FM3-38, 2014, pp. 3-7).
  - Sistemas de sistemas, "(…) que incluem pessoas, equipamentos e instalações que oferecem conectividade de comunicação de ponta a ponta para componentes de rede (…)"[12] (FM3-38, 2014, pp. 3-8).
  - Serviços de informação, que permitem "(…) coletar, processar, armazenar, transmitir, exibir e disseminar informações (…)"[12] (FM3-38, 2014, pp. 3-8).

Estas operações no ciberespaço são materializadas num conjunto de ações:

- *Cyberspace attack* - ações no ciberespaço que são preferencialmente empregues em apoio a OCO (FM3-38, 2014, pp. 3-3), criando vários efeitos de negação direta no ciberespaço (*Deny*) e manipulação (*Manipulate*) (Joint Publication 3-12 (R), 2013, pp. II-5):
  - *Deny*, que é impedir o uso adverso de recursos, degradando (*Degrade*) uma percentagem, interrompendo (*Disrupt*) por um período de tempo ou até mesmo destruindo (*Destroy*) definitivamente a possibilidade do oponente exercer uma operação ou atingir um alvo (Joint Publication 3-12 (R), 2013, pp. II-5).
  - *Manipulate*, que é "controlar ou alterar as informações, os sistemas de informação e/ou as redes do adversário de uma forma que sustente os objetivos do comandante"[12] (Joint Publication 3-12 (R), 2013, pp. II-5).
- *Cyberspace defense* - são normalmente ações internas no ou através do ciberespaço para proteger, operar e defender a INO (Joint Publication 3-12 (R), 2013, pp. II-4).
- *Cyberspace information collection* - segundo FM3-38 (2014, pp. 3-4), são ações de coleta de informações, que primariamente dão apoio a operações no e através do ciberespaço, através de atividades de vigilância e reconhecimento de redes que podem incluir o acesso e/ou o controle das mesmas, entre outras atividades:
  - *Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR)* - "inclui atividades ISR no ciberespaço conduzidas para reunir informações que podem ser necessárias para apoiar futuras operações, incluindo OCO ou DCO" [12] (Joint Publication 3-12 (R), 2013, pp. II-5);
  - *Cyberspace Operational Preparation of the Environment (OPE)* - embora não sejam ações de coleta de informação, são ações de preparação do ambiente operacional, que incluem identificação dos meios e determinação de vulnerabilidades e planeamento de ações militares de acesso e controle de meios (FM3-38, 2014, pp. 3-5).

[12] Tradução do autor.

Apêndice E - Casos conhecidos

Estónia

A Estónia integrava a União Soviética e em 1991 declarou a sua independência. A iniciativa governamental de diminuir a influência russa (De, 2016) tornou a Estónia num dos países mais desenvolvidos da Europa em matéria de comunicações e sistemas de informação, com reflexos em praticamente todas as áreas da sociedade (Aslanoglu & Tekir, 2012, p. 46).

O Soldado de bronze de Tallinn é um monumento existente na Estónia com significado especial para a Rússia, tendo sido mudado de lugar. Em abril de 2007, a Estónia foi alvo de ciberataques massivos durante 3 semanas (theguardian, 2007). Estes ciberataques foram eficazes ao ponto de inutilizar por algum tempo algumas IC. Embora os ataques não tenham sido reivindicados, a Estónia acusou a Rússia de os ter perpetrado, em resposta à mudança de lugar da estátua do Soldado de bronze de Tallinn.

Foi o primeiro caso de uma ação cibernética mais robusta contra um Estado a ser tornado público, em que foram efetuadas três ondas de ciberataques massivos com objetivos distintos.

"O ataque afetou fortemente toda a infraestrutura de rede; deixando *routers* danificados, tabelas de roteamento alteradas, servidores DNS sobrecarregados, servidores de e-mail com falha. A presidência da Estónia e o seu Parlamento, ministérios do governo do país, partidos políticos, dois maiores bancos, ISP do governo, empresas de telecomunicações experimentaram problemas de interoperabilidade."[13] (Aslanoglu & Tekir, 2012, pp. 46-47).

As autoridades estónias equacionaram invocar o artigo 5.º do Tratado da OTAN. Contudo, segundo o critério de Schmitt, o requisito de gravidade não reunia as condições para ser considerado o uso da força ou ataque armado e não era possível provar o envolvimento de um ator estatal (De, 2016).

Geórgia

No âmbito do conflito da Ossétia do Sul em 2008, mais concretamente entre a Geórgia e a Rússia, a Geórgia foi alvo de ciberataques. Foi a primeira vez que um conflito internacional, político e militar, envolveu operações cibernéticas, pese embora a Rússia tenha recusado a autoria dos ciberataques (The New York Times, 2008).

Comparativamente à Estónia, a Geórgia não era tão avançada em termos de comunicações e sistemas de informação, tendo inclusive uma grande dependência de infraestruturas provenientes da Rússia (Aslanoglu & Tekir, 2012, p. 47).

Muitos dos ataques foram similares aos ataques ocorridos anteriormente na Estónia, mas os danos foram maiores, devido essencialmente às fracas e danificadas infraestruturas e à grande dependência dos países vizinhos para conetividade. Após o conflito, a CERT de vários países, incluindo a Estónia, a Polónia e a França, prestaram auxílio à CERT local (Aslanoglu & Tekir, 2012, p. 48).

Embora o Ministro dos Negócios Estrangeiros da Geórgia tenha afirmado que estavam a ser alvo de uma campanha de ciberguerra pela Rússia, o mesmo não foi provado e foi inclusive constatado que muitos servidores usados para os ataques estavam sedeados nos EUA, o que aumentou a dúvida sobre a autoria dos ataques (De, 2016).

Devido a estas dúvidas, à semelhança do que sucedeu no caso estónio, também aqui não se qualificaram os ciberataques como uso da força ou ataque armado (De, 2016).

Stuxnet

O vírus "Stuxnet", que ocorreu em 2010 e que danificou consideravelmente o projeto nuclear do Irão, foi provavelmente a primeira ciberarma sofisticada utilizada num ciberataque (Aslanoglu & Tekir, 2012, p. 49).

Este vírus tinha a particularidade de ser completo e com a liberdade de auto expandir-se. Foi detetado passados vários meses e foi defendido que o sistema iraniano tinha sido infetado via USB. O vírus conseguiu infetar cerca de 60000 computadores espalhados pelo mundo (Aslanoglu & Tekir, 2012, p. 49).

Segundo o grupo de peritos do Manual de Tallinn, o caso do vírus "Stuxnet" compreendia os requisitos do uso da força, mas não havia consenso se estava enquadrado num ataque armado, falhando nos requisitos relativos à iminência e à atribuição, devido a ter sido detetado passado muito tempo e não ser possível atribuir responsabilidade pelo ciberataque (De, 2016).

Estes ciberataques demonstram a necessidade que os Estados têm de se munir de capacidades para exercer operações no ciberespaço, pois existe "em qualquer país, o potencial de acontecerem ataques como os registados" (Farinha & Assunção, 2017). É neste contexto que se enquadram os esforços empreendidos na criação de unidades de ciberdefesa.

[13] Tradução do autor.

Apêndice F - Poder cibernético Mundial

Em 2011, foi efetuado o estudo *Cyber Power Index*, produzido pela *Economist Intelligence Unit* (EIU)[14], com o intuito de criar um benchmarking do poder cibernético mundial a partir de indicadores agrupados em quatro fatores: "(…) quadro legal e regulamentar; contexto econômico e social; infraestrutura de tecnologia; e aplicação da indústria (…)" (Economist Intelligence Unit, 2011, p. 2).

Este estudo compara a capacidade de resiliência de 19 países do G20[15], (com exceção da UE) e considera que os países com índice maior, são os que conseguem equilibrar o elevado grau de dependência do ciberespaço com o consequente aumento dos riscos de segurança (Economist Intelligence Unit, 2011, p. 2). As pontuações dos países são de 0 a 100, em que o Reino Unido tem a maior pontuação (76,8) seguido dos EUA (75,4) e que a China (34,6) e a Rússia (31,7) estão precisamente em 13º e 14º. Portugal não está representado pois não pertence ao G20.

Mais recentemente, em 2015, foi produzido o relatório *Global Cybersecurity Index*, pela *ABI Research* e *International Telecommunication Union* (ITU)[16], com as pontuações entre 0 e 1, em que os EUA tinham a pontuação mais elevada (0,824) e Portugal estava na cauda dos países da Europa, na 19ª posição com 0,294 pontos empatado com outros 8 países (ABI Research, 2015, pp. 1-3).

Richard A. Clarke estimou em 2010, fruto das suas avaliações pessoais, as capacidades de ciberdefesa de alguns Estados, com especial atenção na ciberdependência das infraestruturas críticas (Clarke & Knake, 2010, p. 148). A Tabela 3 demonstra os resultados.

Tabela 3 - Estimativa das capacidades dos EUA e concorrentes ou inimigos

Estados	Capacidade ciberofensiva	Ciberdependência	Capacidade ciberdefensiva	*Score* total
EUA	8	2	1	11
Rússia	7	5	4	16
China	5	4	6	15
Irão	4	5	3	12
Coreia do Norte	2	9	7	18

Fonte: (Clarke & Knake, 2011, p. 148 cit. Fernandes, 2014, p. 114)

É possível verificar que quanto menor é a exposição (maior pontuação em ciberdependência) melhor a capacidade ciberdefensiva, existindo apenas a exceção da China na alta pontuação na capacidade ciberdefensiva, isto por causa da possibilidade de desligar a rede do país inteiro (Clarke & Knake, 2010, p. 149).

Em 2012, foi produzido entre a companhia de segurança McAfee e a *Security & Defence Agenda* um relatório que demonstrou o *ranking* das capacidades de ciberdefesa mais influentes, baseado em entrevistas a individualidades credíveis na matéria, espalhadas pelo mundo (Grauman, 2012, p. 3). A Figura 5 resume o *ranking* produzido.

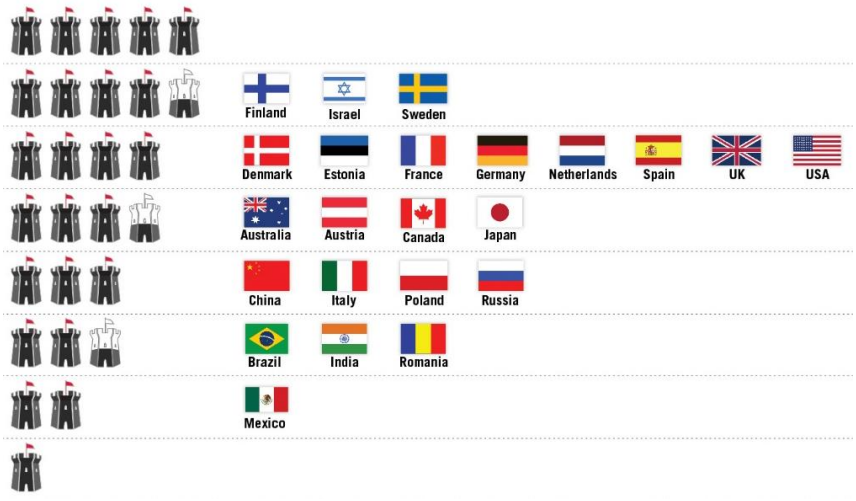

Figura 5 - Rankings de capacidades de ciberdefesa

Fonte: (McAfee, 2012)

[14] EIU "(…) é a divisão de investigação e análise do *The Economist Group* e o líder mundial em *business intelligence* global" (Economist Intelligence Unit, 2017).

[15] G20 são as 20 maiores economias mundiais, que incluem 19 países mais a UE (World Economic Forum, 2016).

[16] ITU "é a agência especializada das Nações Unidas para tecnologias de informação e comunicação" (ITU, 2017).

Apêndice G - Preocupações Internacionais

OTAN

A origem da ciberdefesa na agenda política da OTAN foi em 2002, na cimeira de Praga (OTAN, 2017a). Contudo, apenas em 2008, na cimeira de Bucareste, é que foi aprovada a política de ciberdefesa da aliança (NATO, 2008). No mesmo ano, "(…) a OTAN, acreditou o *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) (...)" (Marinha, 2016, p. 4). O CCDCOE, que está localizado em Tallinn, Estónia, tem como uma das missões, melhorar, na vertente doutrinária, as capacidades de ciberdefesa dos Estados que integram a OTAN e parceiros (CCDCOE, 2015). Nesta altura, a OTAN avaliava a possibilidade de invocar o artigo 5.º em caso de ciberataques (Gallis, 2008). Fruto do esforço do CCDCOE, foi lançado em 2009 o livro académico "Manual Tallinn" (CCDCOE, 2009), que serve de guia sobre a aplicação da lei internacional em conflitos cibernéticos.

Na cimeira da OTAN, em Lisboa, em novembro de 2010, foi aprovado o novo Conceito Estratégico (OTAN, 2010), que revelava a preocupação premente da organização com o número crescente de ciberataques e onde foi destacada a ameaça de ciberataques à segurança, estabilidade e prosperidade nacional e Euro-Atlântica (OTAN, 2010, p. 11), e em 2011, na aprovação da 2ª política de ciberdefesa, os Estados deviam empreender um esforço coordenado no sentido de prevenir ciberataques, aumentar a resiliência e ainda a "integração da ciberdefesa no processo de planeamento da defesa da OTAN"[17] (NATO, 2017b).

Em 2012, a OTAN criou a *Nato Communications and Information Agency* (NCIA), que tem como responsabilidade efetuar operações de ciberdefesa (NCIA, 2012), que incluiu "(…)o centro técnico da NCIRC, fornecendo serviços especializados para prevenir, detetar, responder e recuperar de incidentes de segurança cibernética"[17] (NCIA, 2017).

"Em fevereiro de 2014, os ministros de defesa aliados encarregaram a OTAN de desenvolver uma nova e melhor política de defesa cibernética, em defesa coletiva, assistência aos Aliados, governança simplificada, considerações legais e relações com a indústria"[17], que viria a ser aprovada na conferência de Gales (OTAN, 2017a).

No ano de 2016, a OTAN designou o ciberespaço como um domínio operacional oficial de guerra e estreitou as relações com a UE ao acordar a relação entre a NCIRC e a CERT-EU para melhorar a prevenção e a resposta a ataques cibernéticos. Foram também acordadas medidas para reforçar a participação mútua em exercícios e promoção de pesquisas e treino e a partilha de informações (OTAN, 2017a).

Mais recentemente, começaram em Portugal as obras para edificar a futura *NATO Communications and Information Systems School*, que atualmente está situada em Itália, que proporcionará formação e treino na área da ciberdefesa (Ministro da Defesa Nacional, 2016).

União Europeia

A ciberdefesa tem tido atenção por parte da UE, onde tem procurado criar uma abordagem comum das políticas nacionais sobre esta matéria.

Em 2011, o desenvolvimento das capacidades de ciberdefesa foi incluído nas prioridades da Agência Europeia da Defesa (AED), tendo mesmo sido acordado no ano seguinte o conceito europeu para a ciberdefesa (Parlamento Europeu, 2014).

No ano de 2013, fruto da constatação da incipiente capacidade da ciberdefesa dos Estados membros, a AED recomendou uma série de ações ao nível da UE, que incluíam a melhoria da segurança das redes, o fortalecimento das capacidades de resposta a incidentes, a criação de uma cultura de cibersegurança e o estreitamento das relações com a OTAN. Recomendou também ações ao nível dos Estados membros, tais como o reforço das iniciativas de formação e treino assim como a partilha de informações e conhecimento. Ainda no mesmo ano o Conselho Europeu, definiu o objetivo de no ano seguinte ter uma política de ciberdefesa da UE (Parlamento Europeu, 2014).

Nações Unidas

As NU têm tentado regulamentar o ciberespaço, com o intuito de "desenvolver e manter um ciberespaço pacífico, seguro, estável e previsível"[17], mas para conseguir alcançar os objetivos necessita de abordagens multilaterais (United Nations, 2013, p. 138).

A resolução n.º 58/199, de 2004, convidava as nações mais evoluídas em capacidades no ciberespaço a partilhar e apoiar as outras nações, mas nessa altura havia poucas nações com essas capacidades. Ironicamente 3 destas nações eram membros efetivos do conselho de segurança, os EUA, a Rússia e a China, que já empregavam operações no ciberespaço e com a vantagem que detinham não iam partilhar, nem apoiar outras nações (Global Risk Advisors, 2016).

Os documentos tornados públicos pelo Wikileaks, por Edward Snowden e Bradley Manning (Chelsea Manning), revelaram que agências de segurança norte-americanas "(…) pagam a terceiros (empresas e hackers) por falhas de segurança em sistemas usados por milhões". Assim se justifica que atores internacionais se pronunciem sobre a criação de tratados internacionais sobre o ciberespaço. A "Microsoft defendeu a criação de uma Convenção de Genebra Digital", de modo a proteger os interesses de quem utiliza o ciberespaço (Expresso, 2017).

[17] Tradução do autor.

Apêndice H - Entrevistas

Objetivo: **Entrevista ao CCD**

Entrevistados: Maj/FA Farinha

Capitão-tenente/MAR Assunção

Data da Entrevista: 15/03/2017

A ameaça nacional é real? É possível quantificar o número de ameaças e o número de ataques à nação?

O Centro de Ciberdefesa apenas dispõe de visibilidade sobre as ameaças e número de ataques às redes do universo da Defesa Nacional. Neste momento, o nível de ameaça às Forças Armadas é médio, fruto da combinação entre as ameaças comuns que afetam todos os utilizadores da Internet com as ameaças direcionadas com objetivos de "Intelligence".

No seio dos exercícios/reuniões internacionais, a atual capacidade do CCD é vista com potencial dissuasor? As nossas capacidades estão bem referenciadas? É possível fazer uma comparação com capacidades internacionais?

Estão a ser dados os primeiros passos, no âmbito da NATO, para ser feito um "benchmarking" entre o grau de maturidade das capacidades de ciberdefesa de cada Nação, pelo que neste momento ainda não é possível (nem é intenção) fazer comparações com as capacidades de outros.

Estão estabelecidos acordos/protocolos/convenções com organizações tais como as Nações Unidas, a União Europeia ou a OTAN?

Foi assinado em 2016 um Memorandum of Understanding (MoU) entre o Estado Português (representado pelo EMGFA) e a NATO no âmbito da ciberdefesa, que abrange a troca de informação operacional entre os dois órgãos e as atividades a desenvolver no caso de um eventual pedido de assistência de Portugal à NATO no âmbito de uma crise no ciberespaço.

Existe presentemente necessidade de dotar Portugal de capacidades para operar em contexto de ciberguerra?

Com o reconhecimento durante a cimeira de Varsóvia, em 2016, por parte dos chefes de estado e de governo dos membros da NATO, do Ciberespaço como domínio operacional, é implicitamente criada a necessidade de dotar os membros da NATO com capacidades para conduzir operações militares no Ciberespaço. Essa é uma linha orientadora que, em Portugal, já é identificada na orientação política para a Ciberdefesa: "Implementar a capacidade militar para conduzir todo o espetro de operações no ciberespaço (defensivas, de exploração e ofensivas)" (Despacho n.º 13692/2013 do MDN).

Realçando a crescente ameaça cibernética, o número de recursos humanos definido para o CCD é suficiente? O atual número de recursos humanos colocado no CCD é suficiente ou apenas vai servindo para colmatar as necessidades que vão surgindo? Os recursos humanos colocados no CCD estão capacitados para exercer ciberoperações? Há necessidade de colmatar lacunas através de recursos humanos? Se houver, quais?

A gestão dos recursos humanos na área da ciberdefesa é complexa. O processo de formação de um elemento para o capacitar a executar operações no ciberespaço é longo e requer uma melhor articulação com as respetivas direções de pessoal dos Ramos para garantir uma seleção inicial adequada, de acordo com um conjunto de pré-requisitos essenciais (sem um conjunto sólido de competências de base nas áreas dos sistemas de informação ou redes de computadores, é difícil conseguir atingir uma proficiência considerada suficiente num curto espaço de tempo), e a permanência nas funções mais longa do que é habitual noutras funções militares.

Dado que é uma capacidade "brain-intensive", estão a ser feitos esforços no sentido de adequar o processo de seleção para esta área. Neste processo, a colaboração dos Ramos é essencial.

No que diz respeito ao número de recursos humanos, o módulo fixo do CCD é suficiente para as operações diárias atuais. No entanto, há outras funções a desempenhar, nomeadamente nas áreas de estado-maior, para as quais o módulo atual não foi desenhado e que têm vindo a alocar alguns dos recursos existentes. Para situações de condução de operações no ciberespaço que requeiram um número maior de elementos, está prevista a integração de "augmentees" provenientes das CIRC dos três ramos, que de forma temporária passam a desempenhar as suas funções no CCD. Estes mecanismos de "pulling and sharing" permitem ultrapassar as limitações no módulo de pessoal permanentemente alocado ao Centro de Ciberdefesa. O passo seguinte passará por conseguir identificar pessoal em toda a estrutura das Forças Armadas que possua valências nesta área, para eventualmente poderem reforçar esse módulo de "augmentees" a que o Centro de Ciberdefesa possa recorrer quando necessário.

O CCD tem as ferramentas/meios necessários para exercer ciberoperações?

O CCD tem vindo, desde 2014, a equipar-se com as ferramentas e meios materiais necessários à condução de operações no Ciberespaço. Algumas das ferramentas dependem especificamente da missão a executar, pelo que poderá não fazer sentido fazer uma acumulação de meios, sem saber concretamente o tipo de operação específico a desenvolver. Além disso, a acumulação de ferramentas (em particular as ofensivas) não é aplicável na área das operações no ciberespaço, uma vez que rapidamente perdem a sua eficácia operacional (à medida que as vulnerabilidades que exploram vão sendo corrigidas pelos fabricantes de software).

O maior desafio prende-se com os meios humanos, como já explicado acima, em particular em caso de necessidade de operar em formato de força destacada.

As infraestruturas existentes são adequadas ao exercício da missão atribuída?

As limitações existentes nas infraestruturas têm vindo a ser colmatadas com os investimentos realizados desde 2014, pelo que não se considera existirem limitações atuais neste campo.

Temos vulnerabilidades, (de qualquer tipo), que podem e merecem ser colmatadas?

O processo de gestão e mitigação de vulnerabilidades é contínuo, uma vez que estão permanentemente a ser descobertas novas vulnerabilidades nos sistemas de informação em produção e a ser lançadas correções a esses sistemas. As vulnerabilidades também afetam processos e procedimentos, e esses estão a ser alvo de uma avaliação e revisão.

Existem capacidades que merecem ser melhoradas para dotar o CCD de uma capacidade relevante para operar no contexto internacional? A atual estrutura definida para a ciberdefesa, tem capacidade para exercer ciberoperações no contexto internacional?

A execução de operações no ciberespaço será sempre contemplada no plano em que forem conduzidas as operações militares em que estas estão integradas. Uma vez que, por natureza, as operações militares são conduzidas num contexto internacional, as operações militares no ciberespaço não deverão ser diferentes. A capacidade para as executar num determinado cenário terá de ser avaliada caso a caso, considerando a força em que estará inserido e as capacidades e vulnerabilidades da força adversária, pelo que não é possível dar uma resposta genérica.

A atual capacidade de ciberdefesa nacional é considerada pelo poder político? E no contexto de operações militares conjuntas?

A ciberdefesa nacional teve a sua génese na Orientação Política para a Ciberdefesa (do Ministro da Defesa Nacional), de 2013, e é um tema recorrentemente abordado nas esferas políticas (quer a nível nacional, como na NATO). De realçar que ainda em 2016 foi reconhecido pelos chefes de estado e de governo da NATO que o Ciberespaço constitui um domínio de operações militares, e assinado um compromisso (Pledge) sobre a ciberdefesa em que, ao nível político, foram assumidos objetivos comuns a atingir nesta área. Do ponto de vista das operações militares conjuntas, está agora a ser criada a doutrina para a integração das operações no ciberespaço com as restantes componentes de uma operação militar. A NATO está a desenvolver o AJP 3-20 "Allied Joint Doctrine for Cyberspace Operations", que visa estabelecer uma primeira abordagem a essa integração.

Uma possível junção/partilha de qualquer tipo de recursos com o centro nacional de cibersegurança é viável?

A partilha de informação (que é também ela um recurso importantíssimo na área da cibersegurança) é um exemplo já tornado realidade com o CNCS, e é imprescindível para o aumento da segurança no ciberespaço.

Do ponto de junção de recursos, as missões do Centro de Ciberdefesa e do CNCS são significativamente diferentes, pelo que poderia não haver uma mais-valia nessa junção.

De qualquer forma, está prevista na lei orgânica do EMGFA a cooperação com o CNCS no âmbito da cibersegurança setorial da defesa nacional, ao que não se exclui a partilha de recursos ou até disponibilização de apoio por parte do CCD em caso de ser necessário fazer face a uma situação de crise para a qual o CNCS não tenha recursos suficientes.

Segundo alguns estudos, a estratégia Chinesa passa por utilizar hackers referenciados pelo governo, para exercer ciberoperações, era viável uma solução idêntica em Portugal?

Não conhecendo o teor dos estudos referidos, aquilo que é possível afirmar é que teria de ser avaliado, do ponto de vista jurídico, o estatuto aplicável a um civil que conduza operações militares no ciberespaço, nomeadamente a proteção aplicável ao abrigo do estatuto de combatente. Essa análise não foi ainda desenvolvida.

Questões técnicas, jurídicas (nacionais e internacionais) e políticas, limitam as ciberoperações?

Os aspetos técnicos, jurídicos e políticos estabelecem sempre limites, em qualquer domínio operacional em que as Forças Armadas Portuguesas operem. Cabe ao comandante da força avaliar as limitações e desenhar a operação militar de forma a minimizar o impacto dessas limitações.

As nossas infraestruturas críticas estão salvaguardadas de ciberataques?

Considerando a expressão "nossas" como "Forças Armadas", as infraestruturas críticas são salvaguardadas tendo em linha de conta as boas práticas na implementação de sistemas de informação que são seguidas pelos Ramos. Não há, contudo, uma metodologia formal para a análise de risco associada à implementação dos sistemas de informação associados a essas infraestruturas críticas.

Do ponto de vista das infraestruturas críticas nacionais, o Centro de Ciberdefesa não tem informação relevante, sendo essa uma competência do CNCS.

Ataques como os que aconteceram na Estónia ou na Geórgia podem acontecer em Portugal?

Existe, em qualquer país, o potencial de acontecerem ataques como os registados na Estónia ou na Geórgia. No entanto, esse potencial deve ser sempre analisado tendo em conta a existência (ou não) de uma força opositora que tenha interesse em desenvolver um ataque desse tipo.

Do ponto de vista das potenciais consequências, uma vez que estamos a falar de um ataque maioritariamente sobre entidades da Administração Pública e Infraestruturas Críticas Nacionais, a entidade competente para responder a essa pergunta é o CNCS.

Serviço: **Entrevista ao Consultor Coordenador do Departamento de Operações do CNCS**

Entrevistados: Maj/GNR Raposo

Data da Entrevista: 24/03/2017

A ameaça nacional é real? É possível quantificar o número de ameaças e o número de ataques à nação?

É real, mas não completamente desconhecida. Não é viável a produção atual de uma estatística realista, pois muitas entidades resolvem as situações internamente sem as comunicarem. Desta forma apenas temos conhecimento dos casos muito graves, de incidentes que detetamos ou os casos que afetam mais que a própria entidade ou até mesmo outro Estado.

Estão estabelecidos acordos/protocolos/convenções com organizações tais como as Nações Unidas, a União Europeia ou a OTAN?

Há a Diretiva NIS da União Europeia, que é uma legislação sobre cibersegurança que também influi num aumento da cooperação entre Estados. Estabelece regras e irá comprometer os operadores dos serviços essenciais, quer sejam energia, transporte, saúde e outros, a possuírem alguma capacidade de segurança sobre os seus serviços digitais. Determinou a criação da rede europeia de equipas de resposta a incidentes de segurança informática (CSIRT), composta por CSIRT dos Estados-Membros, onde o Centro Nacional de Cibersegurança (CNCS) representa Portugal e é o ponto de contato único Nacional encarregue de entrar em contato com os pontos de contacto únicos dos outros Estados-Membros.

No âmbito da OTAN há um memorando de entendimento que é assegurado, na componente nacional, pelo Centro de Ciberdefesa do EMGFA.

Uma possível junção/partilha de qualquer tipo de recursos (materiais ou humanos) ou até mesmo a existência de um edifício único com o centro de ciberdefesa traria vantagens?

Os âmbitos são diferentes.

Os Estados têm que confiar uns nos outros para partilhar informação, porque é sensível. As entidades tendem a confiar primariamente naquelas com quem mantêm relações de afinidade, quer seja de negócio ou da sua natureza. Em Cibersegurança a linguagem não é muito distinta (ou quase nada) independentemente da natureza das entidades, porque o ciberespaço é um espaço comum que a todos afeta e em todos impacta. A localização de diversas entidades relacionadas com a Cibersegurança num único espaço não iria influenciar o âmbito das suas atribuições e talvez criasse um ambiente propício a uma maior proximidade, mas o local físico onde os "centros" se encontram não é determinante nem é impeditivo de que as entidades confiem uma nas outras e partilhem experiências e informação para um objetivo comum.

O CNCS é uma entidade civil que quer que as empresas partilhem informação voluntariamente e possui um protocolo de cooperação e partilha de informação com o Centro de Ciberdefesa.

As nossas infraestruturas críticas estão salvaguardadas de ciberataques?

A salvaguarda que existe é a exigência de comportamentos e medidas de segurança. As infraestruturas críticas possuem os seus órgãos de gestão e a segurança é algo que normalmente está na "lista" das suas prioridades. Há uma atenção especial do CNCS às mesmas, independentemente de possuírem uma natureza pública ou privada.

Está pensado algum tipo de formação escolar ao nível académico não superior com o enfoque na precaução e segurança no ciberespaço?

Está referido na alínea b) do nº1 do Artigo 2.º-A do Decreto-Lei n.º 69/2014 de 9 de maio, que o CNCS deve procurar "promover a formação e a qualificação dos recursos humanos na área da cibersegurança com vista à formação de uma comunidade de conhecimento e uma cultura nacional de cibersegurança". Neste sentido tem havido formação nesta área, promovida pelo CNCS, e um conjunto de iniciativas de apoio ou parceria com outras entidades nacionais com responsabilidades ao nível da educação e formação.

A formação escolar ao nível académico não superior é uma vertente que é também explorada, mas existência de uma disciplina de cibersegurança ao nível dos vários níveis de ensino obrigará a um planeamento cuidadoso a vários níveis, como por exemplo o seu impacto nos horários. Talvez implique uma alteração dos currículos que altere disciplinas e isso terá um impacto ao nível do corpo docente escolar, por exemplo. São questões que não são fáceis de resolver, mas que devem ser pensadas para que se possa melhorar a resiliência digital do país.

Um bom exemplo foi a criação, no ano passado, de currículos de cursos técnicos para especialistas em cibersegurança, que não haviam em Portugal.

Serviço: **Entrevista ao Coordenador Jurídico do CNCS**

Entrevistados: Maj/FA Leite

Data da Entrevista: 24/03/2017

Sendo a ciberguerra uma nova dimensão da guerra, resultante de avanços tecnológicos inexistentes na altura da elaboração das normas de Direito Internacional Humanitário (DIH)/Direito dos Conflitos Armados (DCA) hoje em vigor, pode (deve) ser legalmente regulada pelo DIH/DCA existente, ou há divergências ou um vazio jurídico?

Quando o espaço aéreo começou a ser utilizado como domínio para a realização de operações no decurso de conflitos armados, foi discutido se deveria haver um tratado internacional para regular as questões da guerra aérea.

Em consequência as Nações reuniram-se numa conferência internacional em 1923 em Haia para discutir as eventuais regras a incluir num novo tratado internacional. Chegaram a acordo relativamente a um texto só que esse tratado nunca entrou em vigor enquanto direito internacional oriundo de convenções internacionais. Algumas das regras constantes desse texto entraram depois em vigor, mas como costume internacional. E mais tarde algumas dessas regras foram introduzidas em disposições em convenções internacionais.

O que é um facto é que temos vivido desde essa altura sem demasiada exigência dos Estados na adoção do referido tratado. Têm existido conflitos armados, o poder aéreo tem sido utilizado de forma expressiva e não se verificou a necessidade de regulamentar de forma adicional esta matéria.

Não existe qualquer vazio jurídico. Aquilo que se utiliza é o Direito Internacional em vigor, de natureza geral e interpretá-lo com as devidas adaptações ao domínio do ciberespaço. Existe um Grupo Governamental de Peritos no seio das Nações Unidas que declarou que ao ciberespaço aplica-se o Direito Internacional.

Deste modo, é necessário ao aplicador do direito adaptar as regras que existem ao ciberespaço. Até agora não houve vontade dos Estados de chegar a um consenso relativamente a um tratado sobre Ciberguerra por exemplo, nem é expectável que venha a haver, porque as grandes potências não têm um entendimento consensual por razões várias (paridade estratégica ou falta dela, modelo de sociedade e relacionamento deste com o ciberespaço, etc.). O Direito Internacional depende em grande medida dos Estados e estes prosseguem o interesse nacional pelo que procuram em cada momento aquilo que melhor serve o seu interesse nacional e neste momento isso não passa pela celebração de um tratado.

Outra situação é que em regra, infelizmente, o Direito Internacional Humanitário está sempre "com uma guerra de atraso" pelo que ainda não conseguimos vislumbrar em toda a sua extensão todas as situações que importa regular neste contexto.

Poderá ou estará a ser considerada nas Nações Unidas uma convenção internacional específica no contexto do ciberespaço?

Ver resposta anterior.

Há algumas iniciativas em curso e não só no seio das Nações Unidas. Por exemplo, a Microsoft está bastante empenhada no desenvolvimento de normas do Direito Internacional. Outras empresas neste âmbito também têm demonstrado interesse neste assunto. Há também o denominado "Manual Tallinn" que constitui legalmente mera doutrina, mas que constitui um excelente instrumento de diálogo jurídico menos sujeito a constrangimentos decorrentes do desenvolvimento de políticas sujeitas ao interesse nacional.

Atualmente, em que circunstâncias um determinado ciberataque pode ser considerado um ato de guerra? Tem de ser entre Estados?

Como referido anteriormente, na ausência de uma norma específica relativamente ao ciberespaço teremos que utilizar o direito existente e utilizá-lo com as devidas adaptações.

Um ciberataque pode ser considerado um ato de guerra se as respetivas consequências constituírem uso da força seguindo o critério da escala e dos efeitos.

Este critério ficou estabelecido no processo denominado "Atividades militares e paramilitares na Nicarágua", que opôs a Nicarágua e os Estados Unidos da América, decidido pelo Tribunal Internacional de Justiça em 1986.

Em termos de Direito Internacional o uso da força só pode ser perpetrado por atores Estatais.

Relembrando a decisão do caso da Nicarágua (27 de junho de 1986) e também os ciberataques efetuados à Estónia (27 de abril de 2007), um ciberataque efetuado a um estado por cibernautas (não estatais) de outro estado, pode ser considerado um ato de guerra e justificar/legalizar o uso da força (Jus ad bellum)?

Um ciberataque efetuado a um Estado por indivíduos de outro Estado só pode ser considerado um ato de guerra e justificar o uso da força se esses indivíduos estiverem sob autoridade e direção do Estado em questão.

Em que circunstâncias cibernéticas é justificado/legalizado o uso da força (Jus ad bellum)?

Ação ao abrigo do Capítulo VII da Carta das Nações Unidas ou em legítima defesa ao abrigo do artigo 51.º da Carta das Nações Unidas ou ao abrigo do direito consuetudinário.

Os intervenientes numa ciberguerra devem ser tratados de forma similar aos combatentes numa guerra cinética?

Como não existe um tratado específico temos de nos socorrer do Direito Internacional Humanitário que refere quem é que pode ser considerado combatente. Para além de situações dos membros das forças armadas e da situação de "*levée en masse*", há determinados agentes civis que quando acompanham as forças armadas, podem ser considerados combatentes.

Segundo alguns estudos, a estratégia Chinesa passa por utilizar hackers referenciados pelo governo para exercer ciberoperações. No contexto jurídico era viável uma solução idêntica em Portugal?

Em termos de resiliência de uma Nação faz sentido utilizar as capacidades disponíveis na sociedade civil e não só na estrutura militar.

No contexto nacional, podíamos fazer abordagens similares às da Estónia que têm uma "*Cyber Defence League*", em que utilizam as aptidões dos civis que estão a trabalhar durante o ano no privado, mas que se for necessário estão à disposição do interesse nacional. Teria de se equacionar eventualmente efetuar alterações legais para utilizar essa possibilidade.

Em que condições podem as ciberarmas ser legalmente equiparadas a armas físicas e abrangidas por similares restrições às que constam no atual DIH/DCA?

Como não existem limitações específicas tem que se usar o regime geral. O regime geral diz que não podem ser desenvolvidas armas que não cumprem com os princípios basilares da guerra, nomeadamente, o princípio da distinção. Agora saber se, por exemplo, o vírus "Stuxnet" cumpria o princípio da distinção é outra questão. Na minha opinião cumpria, apesar de ter infetado várias infraestruturas críticas a nível mundial, tinha um alvo determinado e o "gatilho" só foi acionado naquele alvo específico, para mim cumpre com o princípio de distinção, mas há pessoas que poderão eventualmente discordar.

O Tratado de Vestefália veio a regular noções e princípios relativos à soberania dos Estados e também relativos a Estados-Nação. No ciberespaço as fronteiras são inexistentes, não há a questão de soberania no ciberespaço, que dificulta o rastreamento de autores de ataques no e sobre o ciberespaço?

Também o ciberespaço está sujeito aos princípios de Direito Internacional. E, o Direito Internacional assenta no princípio da soberania. Portanto se uma infraestrutura estiver num território, em regra é esse País que tem jurisdição sobre aquela infraestrutura.

A Rússia e a China fizeram propostas às Nações Unidas, mas já foram efetuadas propostas às Nações Unidas no sentido de regular um código de conduta no ciberespaço. Esta é uma solução considerada nos fóruns nacionais e internacionais?

É considerada e constitui uma abordagem diferente, mas que não tem vingado.

Qual a relevância do Manual de Tallinn no contexto jurídico nacional relativamente a ocorrências no e sobre o ciberespaço, ou é apenas um manual académico?

O "Manual Tallinn" constitui legalmente mera doutrina, mas é um excelente instrumento para os assessores jurídicos que têm de se debruçar sobre estas questões.

Tabela 4 - Entrevistas das CIRC dos ramos

Entrevistas às CIRC dos Ramos Perguntas	Maj/FA Valente CIRC FA 15/05/2017	CTen/MAR Baptista das Neves CIRC MAR 15/05/2017	Maj/EX Vinagreiro CIRC EX 09/06/2017
As sinergias/articulação entre o CCD e as equipas CIRC dos ramos, (por exemplo os exercícios, formação conjunta e doutrina), possibilitam uma boa preparação, aprimorando a interoperabilidade, para o caso de haver necessidade de desempenhar funções conjuntas? De um modo holístico?	Correto. Toda a experiência de operação eo conjunto efetuada durante os exercícios permite afinar procedimentos e conhecer formas e hábitos de trabalho, as diferentes arquiteturas e as diferentes capacidades especializadas individuais.	Um dos principais problemas que se verificam é uma total ausência de doutrina que enquadre o funcionamento dos Núcleos CIRC e a sua articulação com o CCD. A Marinha por possuir já desde de 2012 uma capacidade própria tem vindo a operar de o Núcleo CIRC muito à semelhança do que fazia através da Capacidade de Resposta a Incidentes de Segurança da Informação (CRISI). O facto de já existir um relacionamento anterior com os oficiais técnicos dos outros Ramos tem facilitado a relação entre os Núcleos (interoperabilidade), no entanto falta definir claramente a Organização e Doutrina que suporta a Capacidade de Ciberdefesa. Têm existido algumas (muito poucas) oportunidades de formação conjunta e ao nível de Treino a única oportunidade tem sido a participação conjunta do exercício Nato Cyber Coalition, mas que na prática não se identifica com o modo como operamos diariamente.	Sim. Atualmente o CCD/EMGFA participa em Exercícios internacionais no âmbito da NATO e o Exército tem sido convidado a participar. Por outro lado, o Exército lidera o único exercício Nacional de Ciberdefesa (série CIBER PERSEU) que, para além de todas as entidades militares, convida a participar outros organismos públicos e entidades nacionais. As sinergias e a experiência que daqui resultam são fundamentais para o desempenho de funções conjuntas nesta área. Para além dos exercícios, o Exército reconhece que tem havido uma preocupação por parte do CCD/EMGFA em organizar formações para os Ramos que sem dúvidas contribuem para o "conjunto".
O atual número de recursos humanos, (do CCD e as equipas CIRC dos ramos), é suficiente e capacitado para operar em contexto de ciberguerra?	Na minha opinião, Não. No meu entendimento, ciberguerra consiste no uso armado do ciberespaço para obter vantagem sobre o adversário. A esta escala estaremos naturalmente a falar de ataques diferenciados com diferentes alvos e diferentes metodologias. Os elementos especializados em ciberdefesa não são suficientes para as operações ofensivas e defensivas necessárias para travar uma ciberguerra.	O Caso do CCD é distinto dos Ramos, pois por altura da sua edificação foi logo estabelecido um quadro mínimo de pessoal, tendo sido guarnecido com Oficiais Superiores, Subalternos e sargentos vindos dos Ramos. No Caso dos Ramos estes recorreram aos oficiais que de algum modo já estavam ligados à área de segurança. No caso específico da Marinha existem apenas dois (um oficial superior e um subalterno) que respondem pela manutenção da CRISI e pela operação do Núcleo CIRC, apesar de apoiados por dois técnicos de servicedesk, o numero é manifestamente insuficiente face à necessidade de acumulação de funções.	Creio que não. Compreendemos que não é um problema exclusivo desta área, contudo o grau de aprendizagem e especificidade técnica, não é compatível com a gestão de pessoal que é feita nas Forças Armadas e em particular no Exército. - Os Quadros orgânicos estão subdimensionados e são muito específicos em relação aos postos a ocupar, havendo a probabilidade de se perderem talentos só porque não existe cabimento orgânico para determinado posto; - Elevada rotatividade devida a escalas de deslocamento; - Baixa taxa de recrutamento. Estas áreas começam a ser muito bem remuneradas no mundo civil;
Existem capacidades que merecem ser melhoradas para dotar a atual capacidade de ciberdefesa nacional de uma capacidade relevante para operar no contexto internacional? Mais concretamente ao nível da doutrina, treino, formação, recursos humanos, material, infraestruturas e interoperabilidade?	As principais capacidades a serem exploradas estão elencadas na pergunta. Falta uma melhoria na doutrina, no treino, na formação especializada, e na quantidade de recursos humanos disponíveis. A principal lacuna neste momento na minha opinião é Doutrina e Organização.	Considerando o modelo NATO de edificação de capacidades DOTMLPII, como referi anteriormente está ainda quase tudo por fazer. Apenas ao nível de Material, Infraestruturas e Interoperabilidade existe algo de concreto, sentindo-se a necessidade de edificar uma Doutrina que enquadre a Capacidade e uma Organização que a suporte. O Pessoal continua a ser o maior problema, verificando uma grande ausência de recursos humanos qualificados e treinados para o desempenho das missões de Ciberdefesa. Só fará sentido falar a sério de Treino quando tivermos Pessoal e Organização, talvez por isso seja necessário investir na sensibilização da Liderança.	Desconheço se existe uma estratégia para levantamento de uma verdadeira capacidade de ciberdefesa. O CCD/EMGFA tem adquirido equipamentos, tem formado o seu pessoal e apoiado alguma formação dos ramos, tem participado em exercícios, mas será isto um plano estratégico para o levantamento da capacidade? Os militares que estão a receber esta formação dispendiosa mantém-se na área? Garantidamente no Exército o pessoal que está neste momento colocado no DCSegInfo a qualquer momento é colocado em Santa margarida ou mafra a comandar uma companhia. Esta estratégia deveria comprometer os ramos na gestão que faz os recursos humanos financeiros e materiais.
Haveria vantagens em centralizar e unir os recursos e meios, (humanos e materiais), num comando único? Centralizando assim o CCD e as equipas CIRC dos ramos num espaço único?	Não. Existem vantagens num Comando único para centralizar algumas capacidades, mas mas esse reforço deve ser efetuados com mais recursos humanos e não com os existentes. As equipas CIRC dos Ramos terão de existir sempre dado o seu conhecimento local das redes e sistemas e a sua capacidade de intervenção imediata. A alternativa de concentrar todos os recursos deixaria os Ramos sem esta capacidade imediata de reação.	Atendendo às limitações de pessoal que mencionei anteriormente creio verdadeiramente que a centralização das principais valências técnicas no CCD seria muito importante. Na prática os Ramos têm problemas comuns e de algum modo poderiam facilmente geridos de forma centralizada. O que se tem verificado é que na prática quando o CCD precisa de operar como tal, requisita aos Ramos os Técnicos de Cibersegurança/Ciberdefesa dos respetivos Núcleos CIRC para integrarem a equipa do CCD (Exercícios, demonstrações, outras).	Creio que as equipas CIRC são intrínsecas dos Ramos e indissociáveis das especificidades dos SIC de cada um, logo não faz qualquer sentido (minha opinião) concentrar no CCD estas equipas só por questões de proximidade física, contudo não tenho dúvidas que a experiência e o apoio poderia ser potenciado com esta abordagem. No caso do Exército os elementos que constituem as equipas CIRC possuem pessoal em acumulação de funções nomeadamente no apoio a exercícios, grupos de trabalho e uma cadeia hierárquica que não veria com "bons olhos" esta abordagem. Contudo sou da opinião que deveria existir um comando mais "robusto" a um patamar superior, com mais pessoal e uma estratégia bem definida.
Atualmente, quais são os principais desafios?	Os principais desafios da ciberdefesa nas Forças Armadas passam pelo amadurecimento de competências e da afinação da operação dos sistemas de proteção existentes para os tornar mais eficazes. É necessário deixar de reagir a incidentes de ciberdefesa para começar a prevenir estes incidentes. A criação de uma capacidade de operação no ciberespaço através de criação de capacidades de ataque e de exploração constitui também um grande desafio.	A Ciberdefesa tem de rapidamente assumir o seu papel institucional nas capacidades nacionais de Defesa. Para além do controlo sobre o Ciberespaço militar importa alargar os contactos e influência na área mais civil de proteção das infraestruturas e serviços essenciais ao Estado. Não sendo a sua responsabilidade direta, pelo menos em tempo de paz, as FFAA e a Ciberdefesa não podem estar afastadas dos que se passa. Falta, no entanto, o enquadramento Estratégico, a Doutrina e Organização que permitam uma efetiva Ciberdefesa.	Envolver e comprometer os 3 Ramos das Forças Armadas para definição da estratégia a seguir para o desenvolvimento de uma capacidade de ciberdefesa conjunta; Criar Doutrina Nacional; Formar, treinar e Reter talentos nestas áreas (Gestão de pessoal).