INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2012/2013

TII

O *HACKTIVISMO* E AS FORÇAS ARMADAS

DOCUMENTO DE TRABALHO

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

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O *HACKTIVISMO* E AS FORÇAS ARMADAS

Maj Tm David ANTUNES

Trabalho de Investigação Individual do CEMC 12/13

Pedrouços 2013

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

O *HACKTIVISMO* E AS FORÇAS ARMADAS

Maj Tm David ANTUNES

Trabalho de Investigação Individual do CEM-C 12/13

Orientador: TCor Pilav FA António Manuel Gomes Moldão

Pedrouços 2013

Agradecimentos

A realização deste trabalho é um momento marcante do Curso de Estado Maior, só possível quando o esforço individual é revigorado pela ajuda de outros, que cabe agora e aqui, publicamente reconhecer.

Ao meu orientador, Tenente-Coronel António Moldão, pela liberdade que me deu sem nunca deixar de estar atento, disponível e seguro nos conselhos que me transmitiu ao longo do trabalho.

Ao Almirante Gameiro Marques e ao Tenente-Coronel Viegas Nunes, pelos sábios contributos que me guiaram e enriqueceram o trabalho.

Ao Major Gustavo Gapo, e a todos os camaradas que contribuíram de forma direta ou indireta para que este trabalho chegasse ao fim, o meu sincero obrigado.

Uma dedicatória especial:

À minha mulher, Susana, pela sua compreensão, paciência e abnegação.

Ao meu filho, Ivan, que por demasiadas vezes se viu privado da presença do pai e à minha filha Clara, que nasceu no decorrer do Curso e com quem ainda não consegui partilhar todos os momentos que ela merece.

Índice

Índice de Anexos

Índice de Figuras

Índice de Tabelas

Resumo

Este Trabalho de Investigação Individual insere-se no Curso de Estado Maior Conjunto 2012/13 e estuda o papel que podem ter as Forças Armadas portuguesas na cibersegurança nacional. A recente dimensão, o ciberespaço, património comum da Humanidade e novo domínio per si, é um lugar cheio de oportunidades tanto para os indivíduos, as sociedades ou os países que se tornaram dependentes dele. Porém, este mundo virtual apresenta vulnerabilidades que as ciberameaças, onde se inclui o hacktivismo, conseguem aproveitar para conduzir ataques com objetivos diferentes e num alargado espetro de consequências, podendo mesmo levar um estado ao colapso. Não indiferentes a esta realidade, muitos países desenvolveram estratégias orientadas para o ciberespaço, preparando dessa forma estruturas e capacidades capazes de defender e eventualmente ripostar, onde as Forças Armadas dão um importante contributo. As Organizações Internacionais como a Organização do Tratado do Atlântico Norte, a União Europeia ou a Organização das Nações Unidas são relevantes para fomentar a cooperação entre estados para enfrentar as ciberameaças. Portugal tem vindo a despertar para esta nova realidade, desenvolvendo esforços recentes no caminho do estabelecimento de uma estratégia nacional de cibersegurança associada a uma estrutura adequada de resposta e focada num eventual Centro Nacional de Cibersegurança. Demonstramos inequivocamente que as Forças Armadas portuguesas são capazes de contribuir para a cibersegurança nacional em todos os níveis de disrupção levados a cabo por ciberataques. Apresentamos ainda recomendações com medidas concretas para que o contributo das Forças Armadas seja mais efetivo.

Abstract

This Individual Research Paper is part of the Joint Staff Course 2012/13 and studies the role that the Portuguese Armed Forces can play in national cyber security. The latest dimension, cyberspace, a global commons and a new domain itself, is a place full of opportunities for individuals, societies or countries that have become dependent on it. However, this virtual world has vulnerabilities that cyber threats, which include hacktivism, can take advantage of to carry out attacks with different goals and a broad spectrum of consequences, and may even lead to a state collapse. Not indifferent to this reality, many countries have developed strategies for cyberspace, thus prepared structures and capabilities able to defend and eventually fight back, where the armed forces can have an important contribution. International Organizations such as the North Atlantic Treaty Organization, the European Union or the United Nations are relevant to foster cooperation among states in order to tackle cyber threats. Portugal has awakened to this new reality by developing recent efforts for the establishment of a national cyber security strategy linked to a suitable response structure and focused in a probable National Cyber security Centre. We unequivocally demonstrate that the Portuguese Armed Forces are able to contribute to the national cyber security in all levels of disruption undertaken by cyber attacks. We also present recommendations with concrete measures so that the contribution of the Armed Forces can be more effective.

Palavras-Chave

Hacktivismo, ciberdefesa, cibersegurança, ciberespaço, ciberataques, ciberameaças, Forças Armadas, *hackers*, estratégia

Lista de abreviaturas

AED	*European Defence Agency*
ARPANET	*Advanced Research Projects Agency Network*
C2	Comando e Controlo
C4ISR	*Command and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*
CCDCoE	*Cooperative Cyber Defence Centre of Excellence*
CDCM	Centro de Comunicações, de Dados e de Cifra da Marinha
CDMB	*Cyber Defence Management Board*
CEDN	Conceito Estratégico de Defesa Nacional
CEMGFA	Chefe do Estado-Maior-General das Forças Armadas
CERT	*Computer Emergency Response Team*
CFI	*Connected Forces Initiative*
CIRT	*Computer Incident Response Team*
CNA	*Computer Network Attack*
CNCERT	Centro Coordenador da Equipa Técnica de Resposta de Emergência Nacional de Redes de Computadores
CNCSeg	Centro Nacional de Cibersegurança
CNO	*Computer Network Operations*
COTS	*Commercial Off-The-Shelf*
CPNI	Centro para a Proteção das Infraestruturas Nacionais
CRISI	Capacidade de Resposta a Incidentes de Segurança Informática
CRP	Constituição da República Portuguesa
CSM	Conhecimento Situacional Marítimo
CSOC	*Cyber Security Operations Centre*
DAE	Agenda Digital para a Europa
DCEC	*Defence Cyber Expertise Centre*
DCOG	*Defence Cyber Operations Group*
DDOS	*Distributed Denial of Service*
DefCERT	*Defence Computer Emergency Response Team*
DHS	*Department of Homeland Security*
DISS	*Defence Intelligence & Security Service*
DoD	Departamento de Defesa
DPPC	*Defence Policy and Planning Committee*

EC3	*European Cybercrime Centre*
EMGFA	Estado Maior General das Forças Armadas
ENC	Estratégia Nacional de Cibersegurança
ENISA	*European Network and Information Security Agency*
ENSI	Estratégia Nacional da Segurança da Informação
EPR	Entidade Primariamente Responsável
ESCD	*Emerging Security Challenges Division*
EUA	Estados-Unidos de América
EUROPOL	*European Police Office*
FFAA	Forças Armadas
FFSS	Forças de Segurança
FOC	*Full Operational Capability*
GCHQ	Quartel General das Comunicações do Governo
GNS	Gabinete Nacional de Segurança
GPS	*Global Positioning System*
Hi	Hipóteses
IA	*Information Assurance*
IESM	Instituto de Estudos Superiores Militares
IOC	*Initial Operational Capability*
IOP	*Interoperability Point*
ISO	*International Standard Organization*
ITU	*International Telecommunication Union*
JFC	*Joint Forces Command*
LOBOFA	Lei Orgânica de Bases da Organização das Forças Armadas
MIIT	Ministério da Indústria e das Tecnologias da Informação
MIT	*Massachusetts Institute of Technology*
MoD	Ministério da Defesa
NAC	*North Atlantic Council*
NATO	Organização do Tratado do Atlântico Norte
NC3B	NATO *Consultation, Control and Command Board*
NCIA	*NATO's Communications and Information Agency*
NCIRC	NATO *Computer Incident Response Capability*
NCSC	*National Cyber Security Centre*

NCSP	*National Cyber Security Programme*
NL	Holanda
NSA	*National Security Agency*
OCSIA	*Office for Cyber Security and Information Assurance*
ONU	Organização das Nações Unidas
OTSC	Organização do Tratado de Segurança Coletiva
PCSD	Política Comum de Segurança e Defesa
PDE	Publicação Doutrinária do Exército
PDi	Perguntas Derivadas
PIB	Produto Interno Bruto
PM	Primeiro-Ministro
RDE	Rede de Dados do Exército
RPC	República Popular da China
RTE	Rede de Transmissão do Exército
RTm	Regimento de Transmissões
RU	Federação Russa
SCEE	Sistema de Certificação Electrónica do Estado
SGSSI	Secretário-Geral do Sistema de Segurança Interna
SICOM	Sistema Integrado de Comunicações Militares
SIC-Op	Sistema de Informação e Comunicações Operacional
SIC-T	Sistema de Informação e Comunicações Tático
SIED	Serviço de Informações Estratégicas de Defesa
SIEM	*Security Information and Event Management*
SIGINT	*Signal Intelligence*
SIRP	Serviços de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
SPIIN	Sistema de Proteção da Infraestrutura de Informação Nacional
TACOMS	*Tactical Communications Post-2000*
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
UK	Reino Unido
USCYBERCOMMAND	*US Cyber Command*
USSTRATCOM	*United States Strategic Command*

Introdução

Aos domínios da guerra tradicionais, como o marítimo, terrestre, aéreo e espacial, junta-se na atualidade um quinto, o ciberespaço. Este constitui-se como um cenário para novos desafios, onde se podem desenvolver todo o tipo de atividades num mundo virtual com consequências bem reais, alavancadas pelas caraterísticas únicas deste novo ambiente.

Criada inicialmente para fins militares, esta rede global, denominada Internet, é o palco de atividades que visam o bem estar, o desenvolvimento económico, a troca de informação, mas onde abundam também outras intenções.

Assistimos diariamente ao aparecimento de novo *malware*, isto é, software que procura danificar computadores ou sistemas, com tendência para um aumento acentuado. A palavra inglesa *hacking* refere-se à utilização de uma ferramenta para um fim diferente daquele que foi originalmente desenvolvida. Os *hackers*, no domínio cibernético, são motivados por razões ideológicas, de desafio e reconhecimento na comunidade e cada vez mais por motivos financeiros. Quando a técnica de *hacking* procura atingir objetivos políticos, estamos na presença de *hacktivismo*. Apesar da aparente clareza da definição, neste tipo de atividade nada é claro e facilmente se confunde o ciberativismo social e político com vandalismo ou ciberterrorismo. Como exemplos, basta observar que na invasão do Iraque, alguns *sites* governamentais dos Estados Unidos da América (EUA) foram modificados, num claro protesto contra a guerra e incitando à recreação; os apoiantes de Julian Assange (fundador do *Wikileaks*), lançaram ataques contra instituições de crédito; os vários episódios ocorridos durante a Primavera Árabe, em que entidades governamentais e *hackers* apoiantes da democracia se digladiaram na internet. Grupos organizados, organizações internacionais ou países podem patrocinar o *hacktivismo* neutralizando ou danificando profundamente as infraestruturas críticas de um estado. É neste tipo de contexto que este trabalho pretende centrar o seu estudo, quando o cenário transcende a capacidade das operadoras de telecomunicações, das Forças de Segurança (FFSS) em que o poder disruptivo é de tal magnitude que precisa do contributo das Forças Armadas (FFAA). Estas poderão desempenhar um papel de enorme relevância, com estruturas para fazer face a esta nova realidade, numa ótica de serviço público e de salvaguarda dos interesses do Estado, assumindo-se como elemento gerador de futuras capacidades partilhadas, no quadro do desenvolvimento de uma futura Estratégia Nacional.

O tema deste trabalho tem o seguinte enunciado: "O *Hacktivismo* e as Forças Armadas". Iremos, nesta fase, definir os conceitos associados ao tema.

- *Hacker*: Termo que apareceu inicialmente no *Massachusetts Institute of Technology* (MIT) e que designa um indivíduo que gosta de explorar os pormenores de sistemas programáveis e alargar as suas capacidades, contrariamente à maioria dos utilizadores, que preferem aprender o mínimo necessário (Raymond, 2000, p.541).
- Ativismo: a participação ativa, direta e militante para conseguir objetivos políticos ou sociais (metac0m, 2003, p.1)
- Forças Armadas: a Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA), indica que "as Forças Armadas Portuguesas são um pilar essencial da Defesa Nacional e constituem a estrutura do Estado que tem como missão fundamental garantir a defesa militar da República" e têm como incumbências "desempenhar todas as missões militares necessárias para garantir a soberania, a independência nacional e a integridade territorial do Estado (...), cooperar com as forças e serviços de segurança (...) no combate a agressões ou ameaças transnacionais" (AR, 2009).

De acordo com o tema proposto, estabelecemos como objeto da investigação o papel das FFAA portuguesas como contribuinte para a cibersegurança do país num cenário de ciberataques disruptivos. A investigação é delimitada às ameaças no domínio do ciberespaço que necessitem a intervenção das FFAA.

A questão central que vai servir de orientação para o desenvolvimento do trabalho é: "Que papel devem ter as FFAA portuguesas como contributo para a cibersegurança nacional?"

Da questão central, foram definidas perguntas derivadas (PDi) e hipóteses (Hi) associadas:

PD1: As ciberameaças poderão ter efeitos disruptivos para um estado?

H1: Existem alguns tipos de ciberataques que podem ser disruptivos para um estado.

PD2: Como organizam outros países e Organizações Internacionais a cibersegurança?

H21: Alguns países desenvolveram estratégias e estruturas de cibersegurança.

H22:Existe cooperação no seio das Organizações Internacionais para enfrentar as ciberameaças.

PD3: Qual o ponto de situação da cibersegurança nacional e que papel atual têm as FFAA?

H31: Portugal despertou para a cibersegurança.

H32: As FFAA portugueses iniciaram o desenvolvimento tímido de uma capacidade defensiva e ofensiva no ciberespaço.

O trabalho irá observar a metodologia estudada na unidade curricular de Métodos de Investigação Científica, que se baseia na abordagem de Raymond Quivy e Luc Campenhoudt utilizada no Instituto de Estudos Superiores Militares (IESM). A investigação será faseada, mas não de forma estanque, podendo haver sobreposição de algumas fases. Inicialmente, explorou-se a literatura disponível e de referência nesta temática. Assistiu-se a conferencias de interesse relacionadas com o tema e conduziram-se algumas entrevistas a entidades de reconhecido saber sobre a cibersegurança.

Foi construído um modelo de análise (Anexo A – Modelo de Análise) a aplicar aos casos de estudo dos países observados. Tem por conceito a "cibersegurança" e três dimensões. Na primeira, "estratégia", procura-se perceber se o país observado já desenvolveu uma estratégia de cibersegurança, desde quando, se está atualizada, quem a elaborou. Elencam-se as ciberameaças que cada país visualiza, com o intuito de reconhecer aquelas que com maior frequência aparecem. Apresentam-se também os pontos principais da estratégia, o que nos ajuda a entender o caminho que o país procura seguir na cibersegurança. Para a dimensão "entidades responsáveis", são analisadas as estruturas públicas e eventualmente privadas que são responsáveis pela cibersegurança, de forma a identificar diferentes possibilidades de organizar a resposta de um país às ciberameaças. Para a dimensão "contributos das FFAA", procura-se particularizar a análise às FFAA, investigando a estrutura, a forma de colaboração com outros setores da sociedade, e eventualmente efetivos e a maturidade da capacidade de ciberdefesa do país.

Toda a informação recolhida nos passos anteriores ou nas entrevistas será analisada e comparada com a realidade nacional, para serem apresentadas conclusões/recomendações.

O trabalho está dividido em quatro capítulos. No primeiro capítulo, define-se o ciberespaço e demonstra-se que, como património comum da Humanidade, é atualmente considerado um novo domínio. Veremos como estamos cada vez mais dependentes do ciberespaço e, do mesmo modo que este é fonte de progresso onde se desenvolvem múltiplas atividades, outros atores procuram, através da tecnologia, atingir um objetivo e tirar uma vantagem. Apresentam-se situações onde as ciberameaças se tornaram efetivas, sendo por isto necessário a preparação preventiva e a resiliência. No segunda capítulo procura-se analisar o que outros países têm vindo a realizar no âmbito da cibersegurança,

sendo para o efeito sido selecionados cinco países como casos de estudo: Estados Unidos da América, Holanda, Federação Russa, República Popular da China e o Reino Unido. A cada país aplicou-se o modelo de análise, procurando retirar um padrão comum que possa ser útil para a nossa realidade nacional.

O terceiro capítulo debruça-se sobre Organizações Internacionais das quais Portugal é membro, tendo por isso responsabilidades de cooperação mas também onde algumas boas oportunidades podem surgir. Assim, veremos a resposta da cibersegurança na Organização do Tratado do Atlântico, na União Europeia e na Organização das Nações Unidas.

No quarto capítulo, focamos a nossa atenção no caso nacional, efetuando um ponto de situação atual sobre a cibersegurança, analisando os documentos mais recentes que apontam para o desenvolvimento de uma ciberestratégia, quais as entidades responsáveis criadas, por criar e o papel particular das FFAA.

1. A problemática das ciberameaças

"However absorbed a commander may be in the elaboration of his own thoughts, it is sometimes necessary to take the enemy into consideration."

Winston Churchill, 1874-1965

a. O ciberespaço como novo domínio

Ciberespaço, termo que aparece originalmente num livro de ficção científica em 1984, *Neuromancer*, de William Gibson, é definido pela Porto Editora como o "espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações". A *International Standard Organization* (ISO), vai mais longe, definindo-o como "um ambiento complexo que resulta da interação das pessoas, *software* e serviços na Internet, suportado pela distribuição mundial de equipamentos e redes de informação física e tecnologias de informação" (ISO, 2012)

O ciberespaço é hoje visto, por vários autores, como um dos patrimónios comuns da Humanidade, a par com o alto mar, o espaço aéreo internacional e o espaço; um bem público e universal que, não sendo propriedade de nenhum estado, precisa de ser livre e estável para o bem do sistema internacional moderno (CNAS, 2013). Estes quatro *global commons* encontram-se interligados e a sua prosperidade e acesso são uma necessidade económica e militar (ACT, 2013), cuja governação precisa de ser regulamentada através de tratados internacionais. É o caso, por exemplo, da Convenção das Nações Unidas sobre o Direito do Mar. No que diz respeito ao "jovem" ciberespaço, porém, muito caminho resta a percorrer relativamente à elaboração de um código de conduta internacional.

Alguns intelectuais pensaram sobre a importância destes patrimónios comuns da Humanidade, nomeadamente na relação que um país deve manter com eles e no que diz respeito ao uso militar em particular. Alfred Mahan, por exemplo, influenciou a marinha a partir de 1890 com uma obra literária que apelava à possessão do mar, assegurando assim qualquer vitória e sucessos estratégicos, visto que os oceanos eram o palco do comércio e ofereciam inúmeras possibilidades às nações. Neste sentido, era fundamental dispor de uma marinha capaz de destruir o adversário e controlar o mar. Giulio Douhet, por seu lado, defendia no início do século passado, que o "ar" seria algo a ser atravessado a fim de chegar ao coração do território inimigo, pelo que apoiava a indústria aeronáutica no intuito de conseguir uma força aérea forte, capaz de assegurar o acesso ao domínio aéreo (Vacca, 2011, p.164). Olhando para a maior potência à escala mundial, Barry Posen afirma que o comando destes patrimónios globais é "a chave militar facilitadora do poder global dos

EUA (...) que permite explorar a fundo outras formas de poder, como o económico (...) e contribuir para um potencial militar mais útil para alcançar uma política externa hegemônica" (Posen, 2003, pp.8-9). Nesta linha de raciocínio, importa operacionalizar estes domínios, algo que o Homem tem vindo a fazer ao longo da História.

Começou-se a operacionalizar o domínio "terrestre", e com os primeiros navios nasceu o domínio "marítimo". No início do século passado, surgiu o domínio "ar" e só mais recentemente, o domínio "espaço". Será que a nova dimensão "ciberespaço", da autoria do Homem, pode ser considerada um novo domínio? Existe algum debate sobre a matéria, com visões opostas. Libicki[1] questiona a designação unicamente como justificação do argumento que é necessário desenvolver uma organização, o treino e forças para combater neste ambiente. Não foi preciso, na opinião de Libicki, elevar o espetro eletromagnético a domínio para fundamentar a Guerra Eletrónica (Libicki, 2012). Por outro lado, são cada vez mais numerosas as fontes encontradas na investigação que abordam o ciberespaço como um novo "domínio da guerra". A missão da Força Aérea dos EUA, por exemplo, é "voar, combater e ganhar (...) no ar, espaço e ciberespaço" (US Air Force, 2013). A doutrina conjunta dos EUA reconhece o ciberespaço como um "domínio global dentro do ambiente informacional" (Joint Chiefs of Staff, 2011, p.IV_2). A doutrina nacional, com a Publicação Doutrinária do Exército (PDE) 3.0 "Operações" que afirma que "...os comandantes militares integram as atividades ciber/eletromagnéticas no decurso das operações (...) num domínio do ciberespaço" (Exército Português, 2012).

Todavia, o ciberespaço tem características diferentes dos restantes domínios. É muito barato entrar e deslocar-se nele porque só é preciso um equipamento e uma ligação. É fácil esconder a nossa identidade e localização, conhecer outras pessoas e atuar em conjunto desde lugares diferentes do mundo no mesmo instante. O ciberespaço está em constante crescimento, sempre que uma rede é criada ou a sua largura de banda aumentada ou sempre que uma nova máquina se liga (Shaw, 2010, p.4). Contudo, não tem dimensões físicas, depende unicamente da sua estrutura física composta por elementos de redes (*routers*, *switches*), infraestrutura de transporte (cablagens variada, satélites, redes sem fios) e elementos de informação (servidores).

Hoje, o único domínio construído pelo Homem, o ciberespaço, é palco de oportunidades e desafios, onde as nações podem desenvolver estratégias para se projetar.

b. A dependência do ciberespaço

[1] Cientista sênior da RAND *Corporation* e doutorado pela universidade da Califórnia, Berkeley.

Com a criação do ciberespaço, temos vindo a tornar-nos aos poucos dependentes deste novo domínio. A comunicação esta na essência dos indivíduos e permite a transferência de informação, de ideias ou de sentimentos entre si. Desde cedo, houve pretensões para poder comunicar com "o outro" através de ferramentas capazes de aproximar o que está fisicamente distante. A evolução desta pretensão encontra-se associada ao desenvolvimento das tecnologias de telecomunicações e, como era apanágio em épocas passadas, intimamente ligado aos conflitos militares, motores de avanços tecnológicos.

O passo inicial coincidiu com o aparecimento dos primeiros computadores na década de 1950, inicio da Guerra Fria. Os EUA procuravam uma forma eficiente, descentralizada e resiliente de interligar máquinas, no caso de um ataque nuclear. Nasceu o projeto *Advanced Research Projects Agency Network* (ARPANET), do Departamento de Defesa dos EUA, que é o antepassado da Internet de hoje, método global de comunicação por excelência. Contudo, o ciberespaço é muito mais amplo do que a Internet, pois interliga também outras redes de computadores, por vezes separadas da Internet, como são as redes transacionais de fluxos monetários, do mercado acionista, cartões de crédito e sistemas de controlo de todo o tipo (Clarke, 2010, p.70). As sociedades ocidentais têm alimentado uma adição crescente ao, e no ciberespaço.

Mais de 34% da população mundial utiliza a internet, a qual conheceu um crescimento acima dos 560% entre 2000 e 2012 (Internetworldstats, 2013). Segundo o *McKinsey Global Institute*, as trocas comerciais no ciberespaço ultrapassaram os setores da agricultura ou da energia e a Internet representa em média 3.4% do Produto Interno Bruto (PIB) de 13 países[2], com um crescimento anual importante, responsável pelo aumento de 11% do PIB destes países nos últimos 15 anos. Um estudo de 4.800 pequenas e médias empresas revelou que aquelas com forte presença no ciberespaço, cresceram mais do dobro do que as que não o utilizavam, e criaram também o dobro de empregos. De igual modo, por cada emprego perdido, devido à utilização da Internet, 2.6 foram criados (MGI, 2011, p.2). Na era industrial do século XIX, foram necessários 50 anos para um aumento de 380 euros do PIB *per capita*. Países com forte maturidade no ciberespaço conseguiram o mesmo aumento em menos de 15 anos (MGI, 2011, p.3).

Além do impacto económico, a nível social as mudanças são também visíveis. Lemos hoje muito menos em suporte papel revistas, livros e jornais; passamos menos

[2] Países do G8, China, Índia, Brasil, Suécia, Coreia do Sul.

tempo em frente à televisão e ouvimos menos a rádio porque dedicamos mais tempo a jogar *online*, enviar mensagens, participar em redes sociais ou até utilizar serviços de videochamadas com familiares e amigos. A forma como aprendemos sofreu uma verdadeira revolução: utilizamos *software* especializado, assistimos a formações pré-gravadas, lemos blogues, acedemos a livrarias virtuais,.... tudo disponível na *World Wide Web*. Existem *websites* de todos os tipos: tecnológicos, políticos, sociais, comerciais, etc. num mundo virtual, sem fronteiras que nos permite criar, partilhar e interagir. Olhando para o exemplo das vidas nos países do ocidente, é óbvia a influência que tem hoje o ciberespaço em comparação com duas décadas atrás.

Se o ciberespaço nasceu por uma necessidade militar, não deixou de ter mais tarde um impacto a nível global, criando uma grande dependência, sobretudo em países tecnologicamente mais desenvolvidos. Os sistemas de Comando e Controlo modernos precisam do espetro eletromagnético disponível e de redes de telecomunicações seguras para a propagação de voz e dados. No ciberespaço abundam fontes abertas disponibilizadas por múltiplos autores e que são utilizadas pelas Informações militares, e através deste mundo virtual, é possível a troca e armazenamento de informações. Alguns fogos não letais podem ser aplicados através do ciberespaço, numa vertente ofensiva, causando danos que podem ser importantes, como aqueles verificados pela Geórgia às suas Infraestruturas Críticas de Informação em 2009, que deixou o país impossibilitado de comunicar com o exterior. As forças atuais, no seu movimento e manobra, utilizam o *Global Positioning System* (GPS) ou sistema equivalente para a navegação, que assenta em comunicações por satélite e outras redes de telecomunicações que podem ser empasteladas. A proteção da força resulta também de uma adequada proteção do ciberespaço, negando ao inimigo informação sobre as nossas forças. Como último exemplo relacionado com as funções de combate, a logística utiliza o ciberespaço para monitorizar deslocamentos e compras de abastecimentos (Crowell, 2012).

Observa-se outro facto nas aquisições de equipamentos para fins militares: cada vez mais são comprados equipamentos *Commercial Off-The-Shelf* (COTS), ou seja de uso não exclusivamente militar, disponível para o público em geral. Acontece por dois motivos principais: um de ordem económica, porque os orçamentos são mais reduzidos, afirmação que assume maior relevância em tempos de crises económicas e a aquisição de material em uso no mundo civil torna-se mais vantajosa devido à economia de escala. Outro de ordem técnica, porque é difícil acompanhar o avanço tecnológico do mundo civil, o que tornaria obsoleto e oneroso desenvolver e fabricar material especificamente para uso militar. A

maioria dos equipamentos eletrónicos são construídos em países como a China. Podemos especular num cenário onde, no processo de fabrico, seriam inseridas linhas de código malignas no *hardware* dos equipamentos, pelo que deve ser garantida a confiança com o fabricante.

Mas tanta conexão com o ciberespaço criou igualmente um sem número de novos problemas, desde a sua dependência às fragilidades dos sistemas, que podem ser aproveitadas por atores mal intencionados que lhe acedem tão facilmente como outros, abrindo um leque de oportunidades.

c. As ciberameaças

Uma ameaça é qualquer perigo potencial para a informação ou para os sistemas, que ocorre quando algo ou alguém identifica uma vulnerabilidade específica e a utiliza (Harris, 2010, p.54). Não se trata de nada de inovador, pois as ameaças no ciberespaço são parecidas com aquelas que conhecemos no mundo real, tais como: crime, espionagem, ativismo, terrorismo (Robinson et al., 2013, p.5).

Cada nação carateriza as ciberameaças de forma distinta, não existindo uma definição comum. Contudo, podemos diferenciá-las utilizando a metodologia da *International Telecommunication Union* (ITU), que as classifica segundo as suas caraterísticas, impactos, origens e atores: podem ser "acidentais", se não houve premeditação, por exemplo no caso de uma falha de *software* involuntária; serão "intencionais", com vários graus de sofisticação, sempre que exista uma vontade de atacar; as ameaças "ativas" modificam o estado ou operação de um sistema enquanto que as "passivas" não afetam o sistema, mas recolhem informação (Wamala, 2011). Em relação à origem, são reconhecidas três tipologias de atores diferentes, como fontes das ciberameaças, divididas em vários subtipos e objetivos, de acordo com um estudo elaborado por Khalilzad em 1998, que continua atual:

Tabela 1 - Tipologia de ameaças

Fonte: adaptado de Khalilzad (Robinson et al., 2013, p.6) e ITU (Wamala, 2011, p.16)

Tipo	Subtipo	Objetivos
Indivíduos	*Grey/Black hats* Empregados descontentes	Desordem, vandalismo menor
Grupos coordenados ou redes	Grupos criminais Terroristas Hacktivistas Grupos insurgentes Organizações comerciais	Dinheiro, poder Ganhar apoio / dissuadir a oposição para uma causa Protesto, medo, dor, disrupção. Mudança de um governo ou motivos separatistas Espionagem industrial, venda de informação
Estados	Estados falhados Adversário rival Serviços de Informação	Dissuadir, derrotar ou aumentar o custo de envolvimento de um estado numa disputa regional Dissuadir ou adiar a confrontação, espionagem ou vantagem económica de um país

É também consensual considerarem-se três princípios fundamentais da segurança que são alvo das ciberameaças: disponibilidade, integridade e confidencialidade. A "disponibilidade" consiste em garantir que um sistema se encontra operacional quando pretendemos utilizá-lo. A "integridade" refere-se ao facto da informação não ter sofrido alterações quando armazenada ou no seu percurso, no processo de troca. A "confidencialidade" consiste em salvaguardar o conteúdo da informação. Os ciberataques variam consoante o princípio da segurança que é atingido. Mas até que ponto podem causar danos importantes?

d. Ataques disruptivos

Alguns autores traçam cenários apocalípticos onde os ciberataques têm efeitos devastadores, comparáveis a tragédias como tornados ou tsunamis (Demchak, 2011) (Clarke, 2010). Os ataques cibernéticos podem ser de vários tipos mas aqueles que não envolvem humanos nas suas ações diretas, ou seja conduzidos exclusivamente por máquinas, são ainda mais eficazes, sobretudo quando dirigidos para países menos evoluídos tecnologicamente, como serve de exemplo a disseminação do *worm*[3] *Stuxnet* nas centrais nucleares iranianas em 2010. Contudo, países muito dependentes do ciberespaço podem também sofrer devido à assimetria. A facilidade associada aos desenvolvimentos de ferramentas de *hacking* cada vez mais poderosas e os escassos meios necessários para

[3] verme: software malicioso, semelhante a um vírus, que para além de infectar um determinado sistema se propaga automaticamente para outros nós da rede, infectando assim de forma completamente autónoma um elevado número de sistemas numa rede (CERT.PT, 2012).

conduzir ataques, contrasta com o grande investimento que uma organização ou nação tem que realizar para se defender. A rapidez das comunicações permite hoje um recrutamento fácil de apoiantes, sobretudo em locais mais pobres e estados falhados. Os sistemas críticos complexos, que foram construídos para a prosperidade económica e lazer, são palco de ataques indiscriminados por parte de atores estatais e não estatais, através do globo. Na tabela seguinte, apresentam-se exemplos de ciberataques reconhecidos como dos piores da história, e para os quais existia assimetria entre o potencial atacante e o seu alvo. A informação compilada resulta do cruzamento de dados retirados de páginas da Internet, a fim de encontrar similitudes:

Tabela 2 - Dos piores ciberataques da história

Fonte: adaptado de http://www.dvice.com, (Robinson et al., 2013)

NOME	ALVO	FONTE	DESCRIÇÃO
Moonlight Maze (1998)	Pentágono, NASA, Departamento de Energia	Rússia	Uma das primeiras infiltrações que se conhecem Por um período de dois anos retirou-se informação sensível como mapas, configuração das tropas dos EUA, etc.
Titan Rain (2004)	Empresas, Intel EUA	China	Infiltração em redes sensíveis da Lockheed Martin, NASA e acesso a informações militares
Ciberguerra na Estónia (2007)	Estónia	Grupo de jovens, Nashi	Dos mais conhecidos, demonstrou o quanto um país é vulnerável, ficando paralisando por algumas semanas.
Most serious breach (2010)	Redes militares EUA	Serviços de informação desconhecido	Uma *pen USB* contaminada permitiu a transferência de dados classificados. Catalisador na origem do CYBERCOMMAND dos EUA.

A China é um bom caso de estudo porque, não conseguindo competir ainda com os EUA num conflito armado, procurou desenvolver desde os anos 90 uma capacidade ofensiva cibernética. Para o efeito, incentivou grupos de *hackers* no seio dos seus cidadãos, tem vindo a realizar atividades de ciberespionagem, tomou iniciativas para proteger o seu ciberespaço, (o famoso para-fogo conhecido por "Muro da China") e criou, já em 2003, unidades militares de ciberguerra, capazes de conduzir operações ofensivas e defensivas com ciberarmas tecnologicamente muito avançadas (Clarke, 2010, p.57). O desenvolvimento de capacidades militares simétricas pode ser economicamente esgotante

para um país, como aconteceu por exemplo antes com a *ex* União Soviética. A China segue uma abordagem de "vencer o superior com o inferior", procurando vulnerabilidades críticas no adversário, conhecido como o método de "guerra da acupuntura": um sistema é paralisado ao atacar ou controlar os seus "pontos de energia vitais", os *xue*. Os sistemas C4ISR[4] dos EUA por exemplo, não funcionam sem o ciberespaço e são nele vulneráveis. Consequentemente, é natural que um ator potencialmente mais fraco utilize a tecnologia para colmatar a assimetria operacional (Chen, 2010, p.559). A China ou a Rússia não são casos isolados. Os serviços de informações dos EUA reconhecem que existem à volta de 30 países com capacidades razoáveis para participar numa ciberguerra, como por exemplo, o Irão, a Índia e o Paquistão (Clarke, 2010, p.64).

Arreguín-Toft defende uma teoria interessante que diz que "a melhor profecia do resultado final de um conflito assimétrico deriva da interação estratégica" ou dito de outra forma num corolário, "atores fortes perderão os conflitos assimétricos quando utilizarem uma estratégia errada em relação ao seu adversário" (Arreguín-Toft, 2001, p.95). Assim, é importante possuir uma estratégia de cibersegurança capaz de enfrentar os desafios atuais.

[4] C4ISR –*Comand and Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*

2. A resposta de alguns países

"Na estratégia, decisiva é a aplicação"

Napoleão Bonaparte, 1769 – 1821

Este capítulo visa analisar a postura de alguns países em relação à cibersegurança. A escolha dos países como casos de estudo considerou a sugestão que acompanhou este tema. Assim, analisaremos dois países reconhecidos internacionalmente como muito capazes no ciberespaço, a República Popular da China (RPC) e a Federação Rússa (RU) e três países aliados: os EUA porque são uma referência, o Reino Unido (UK) que desenvolveu um trabalho notável nesta área, destacando-se na Europa e a Holanda (NL), país europeu com dimensões mais próximas de Portugal. Para cada caso, é aplicado, dentro do possível realizar, o modelo de análise apresentado no Anexo A.

Na tabela seguinte, aparecem os valores estimados das capacidades militares de ciberdefesa de uma seleção de países, de acordo com os dados do *Technolytics Institute* onde os valores variam entre o mais baixo (1) e o mais alto (5). Observa-se que no topo da tabela encontram-se a RPC, os EUA e a RU.

Tabela 3 - Capacidade militares de ciberdefesa de alguns países

Fonte: (Melo, 2011, p.14)

Cyber Military Capabilities (2009)	Cyber Capabilities Intent	Offensive Capabilities Rating	Cyber Intelligence Capabilities	Overall Cyber Rating
China	4.2	3.8	4.0	4.0
United States	4.2	3.8	4.0	4.0
Russia	4.3	3.5	3.8	3.9
India	4.0	3.5	3.5	3.7
North Korea	4.2	3.4	3.3	3.6
Japan	3.9	3.3	3.5	3.6
South Korea	3.5	3.0	3.2	3.2
United Kingdom	3.2	3.0	3.0	3.1
Germany	2.5	2.5	2.4	2.5
Brazil	2.1	2.5	2.1	2.2
France	2.0	2.1	2.2	2.1

a. Estados Unidos de América

Vários setores dos EUA dependem do ciberespaço: quer sejam as empresas para os seus negócios, as pessoas a nível social ou até o setor da defesa que opera em mais de 15.000 redes com sete milhões de máquinas instaladas em mais de uma centena de países (Department of Defense, 2011, p.1). Os EUA são o país que mais literatura disponibiliza, de forma livre, onde se sucedem as obras literárias, os artigos de opinião e documentos oficiais relacionados com a cibersegurança (Anexo B).

As ameaças neste âmbito reconhecidas pelos EUA são: nações estrangeiras que pretendam explorar as redes do Departamento de Defesa (DoD), atores não estaduais e atividades ainda não detetadas, atores externos, ameaças internas, vulnerabilidades da cadeia de produção (maior parte dos produtos são fabricados no estrangeiro), e ameaças à capacidade operacional do DoD (Department of Defense, 2011, p.3)

Embora existam estratégias sectoriais diferentes, uma para o Departamento de Segurança Interna (*Department of Homeland Security* - DHS) e outra para o DoD, focaremos a nossa atenção nesta última, até porque o DoD assinou um memorando de entendimento em 2010 com o DHS que espelha a forma como serão "proporcionados meios humanos, equipamentos, instalações a fim de aumentar a colaboração interdepartamental no planeamento estratégico da cibersegurança, o suporte mútuo para o desenvolvimento de capacidades e a sincronização das atividades de missões das operações correntes" (DHS,DoD, 2010).

(1) Estratégia implementada

A Estratégia de cibersegurança do DoD vem expressa em cinco iniciativas estratégicas, sendo a terceira e quarta as mais relevantes para este trabalho uma vez que traduz mais particularmente o contributo do DoD na cibersegurança:

- ✓ " Ver o ciberespaço como um domínio operacional para organizar, treinar e equipar de forma a que o DoD possa retirar plena vantagem no potencial do ciberespaço;
- ✓ Empregar novos conceitos operacionais de defesa para proteger os sistemas e redes do DoD;
- ✓ Ser parceiro de outros departamentos governamentais, agencias e o setor privado pata alcançar uma estratégia global de cibersegurança governamental;
- ✓ Construir relações robustas com os aliados e parceiros internacionais para aumentar a cibersegurança coletiva;
- ✓ Aumentar o talento nacional através se uma força de trabalho cibernética excecional e de uma rápida inovação tecnológica." (Department of Defense, 2011, p.i)

(2) As entidades responsáveis

Os EUA possui uma estrutura organizacional de cibersegurança complexa (Anexo C), compreendendo os seguintes intervenientes:

(a) *National Security Agency*

A Agência de Segurança Nacional (*National Security Agency* – NSA) tem por missão "liderar o governo dos EUA na criptologia que engloba tanto *Signals Intelligence* (SIGINT) e Segurança da Informação (*Information Assurance* – IA) de produtos e serviços, e permite Operações de Redes de Computadores (*Computer Network Operations* - CNO), a fim de ganhar uma vantagem na decisão para a nação e os aliados em todas as circunstâncias" (NSA, 2011).

(b) Departamento de Defesa

O DoD utiliza "o ciberespaço para fins militares, de informações, para os seus negócios, para a movimentação de pessoal e material e para o Comando e Controlo (C2) das operações militares em todo o espetro" (Department of Defense, 2011, p.1). Na prossecução da terceira iniciativa estratégica, o DoD deve trabalhar com o DHS, outras agências e até o setor privado com o qual poderá "partilhar ideias, desenvolver novas capacidades" (Department of Defense, 2011, p.8)

(c) Comando Estratégico dos Estados Unidos

O Comando Estratégico dos EUA (*United States Strategic Command* – USSTRATCOM) foi criado em 1992 e tem por missão "dissuadir ataques sobre interesses vitais dos EUA, assegurar a liberdade de ação no espaço e ciberespaço, proporcionar efeitos cinéticos e não cinéticos (...) em apoio das operações do Comandante das Forças Conjuntas (...)" (USSTRATCOM, 2010).

(d) Cibercomando dos Estados Unidos

O Cibercomando dos EUA (*US Cyber Command* – USCYBERCOMMAND) subordina-se ao USSTRATCOM e à NSA onde está fisicamente colocado, maximizando as potencialidades das duas organizações. É um comando conjunto recente, criado em 2009. Tem por missão "planear, coordenar, integrar, sincronizar e conduzir atividades para: dirigir as operações e defender as redes de informação do DoD; preparar para e conduzir operações militares em todo o espetro no ciberespaço a fim de alcançar ações em todos os domínios, conseguir a liberdade de ação dos EUA e aliados no ciberespaço e negá-la aos adversários" (USSTRATCOM, 2010).

b. Holanda

(1) A estratégia implementada

A estratégia holandesa foi apresentada em 2011 e da análise efetuada ao documento, aparenta ser algo ainda incipiente. São apresentadas seis linhas de ação, onde se refere que NL irá:

- ✓ Assegurar uma abordagem integral por parceiros públicos e privados;
- ✓ Garantir avaliações dos riscos e ameaças atualizadas e apropriadas;
- ✓ Reforçar a resiliência contra disrupções e ciberataques;
- ✓ Reforçar a capacidade de resposta às disrupções e ciberataques;
- ✓ Intensificar a investigação de ciber crimes e a prossecução dos criminosos;
- ✓ Estimular a pesquisa e educação na área da cibersegurança (Ministry of Security and Justice, 2011).

Para a NL, a cibersegurança tem uma "prioridade alta" e as principais ameaças reconhecidas são: estados, organizações privadas, criminosos profissionais, terroristas, hacktivistas, *script kiddies*[5], ciber investigadores e atores internos (NCSC, 2012, p.17).

Esta agenda de trabalho encontra-se num processo de implementação, onde algumas entidades já foram constituídas, como veremos adiante. O setor da defesa emanou em 2012 a sua própria "ciber estratégia".

(2) As entidades responsáveis

A estrutura de cibersegurança holandesa (Anexo D) é constituída pelas seguintes entidades:

(a) *Cyber Security Council*

Operacional desde 30 de Junho de 2011, consiste em representantes de organismos governamentais e empresas que se reúnem para elaborar e implementar uma ciber estratégia. É responsável por aumentar a coordenação de programas de investigação no setor público, privado e instituições como as universidades (NCSC, 2012, p.9).

(b) *National Cyber Security Centre*

O Centro National de Cibersegurança (*National Cyber Security Centre* - NCSC) encontra-se operacional desde 01 de janeiro de 2012 e tem por missão aumentar a resiliência da sociedade holandesa no domínio digital e ajudar a criar uma sociedade da informação estável, livre e segura. É o elo de ligação entre vários organismos, agregando atividades diferentes com vista a conseguir uma maior segurança digital. (NCSC, 2012).

(3) Contributo das Forças Armadas

O ciberespaço é para a NL um quinto domínio das operações militares no qual querem desenvolver esforços em consonância com as três tarefas principais das FFAA: proteção da integridade territorial do reino; promover estabilidade e o respeito das normas

[5] *script kiddies – hackers* com conhecimentos limitados que utilizam técnicas e ferramentas desenvolvidas por outros

internacionais; apoio às autoridades civis na defesa da lei, em desastres e assistência humanitária, a nível interno e internacional. A NL quer ser capaz de "aumentar a sua resiliência cibernética e desenvolver capacidades para conduzir ciber operações". A chave do sucesso é a cooperação transversal, entre o NCSC, os serviços de informações, os serviços de investigação criminal e as FFAA (Ministerie van Defensie, 2012, p.4).

As FFAA desenvolvem elementos defensivo, ofensivo, de informações, inovadores e de cooperação no ciberespaço. O elemento defensivo assegurado pelas *Defence Computer Emergency Response Team* – DefCERT, que se relacionam com outras a nível internacional. O elemento ofensivo é constituído pela *Cyber Task Force*, que pertence ao *Defence Cyber Command* e será responsável por desenvolver doutrina e cenários. O elemento de informações, uma unidade conjunta *cyber*-SIGINT (*Signal Intelligence)* que pertence ao *Defence Intelligence & Security Service* (DISS). Em termos de inovação e adaptação, é criado o *Defence Cyber Expertise Centre* (DCEC) para promover o desenvolvimento, retenção e disseminação do conhecimento. Em relação à cooperação, as FFAA estão representadas no *Cyber Security Council* e no NCSC, "disponíveis para contribuir com conhecimento e capacidades para apoiar as autoridades civis quando solicitadas", de acordo com a lei e uma política de cooperação civil-militar crescente. A nível internacional, procura a troca de conhecimento e mais tarde, o desenvolvimento de técnicas e recursos, essencialmente na NATO e EU (Ministerie van Defensie, 2012, pp.8-16).

c. A Federação Russa

(1) A estratégia implementada

Não existe muita informação disponível sobre a posição russa em relação ao ciberespaço. Um primeiro documento de 2000, " a doutrina de segurança da informação da RU " aborda conceitos relacionados com a deceção e contra informação/propaganda. Em 2009, é emitida a "Estratégia Nacional de Segurança até 2020" da RU. Este documento com 112 pontos estabelece prioridades para a criação de condições de segurança que garantam "liberdades e direitos constitucionais aos seus cidadão, um desenvolvimento estável do país, a preservação da integridade territorial e soberania do estado" e aborda a influencia negativa das atividades ilícitas no domínio cibernético (Decreto Russo, 2009, p.Art 10º) e "as ameaças militares de nações estrangeiras (...) que desenvolvem meios (...) informacionais e de alta tecnologia" (Decreto Russo, 2009, p.Art 30º).

Outro documento mais recente, "Visões conceptuais em relação às atividades das Forças Armadas da Federação Russa no espaço da informação" de 2011, apresenta maior

detalhe. A RU tem uma visão conceptual bastante diferente do ocidente, vendo como fator chave da insegurança a circulação não controlada da informação (Giles, 2012, p.70). Para a sociedade ocidental, a privacidade associa-se a um direito fundamental, como vem expresso, por exemplo, no Artigo 35º da Constituição da República portuguesa. O ciberespaço é aberto e livre mas a Rússia entende que existem exceções: a ameaça da sua utilização para influenciar a esfera sócio-humana (Giles, 2012, p.72).

As ciberoperações merecem um tratamento diferente do que no Ocidente, estando incluídas no mesmo grupo de disciplinas das "guerra da informação", ou seja as Operações de Informação: Guerra Eletrónica, Operações Psicológicas, etc (Giles, 2012, p.74). A RU não pretende copiar as ideias ocidentais, tentando afastar-se de conceitos que não lhe parecem ser aplicáveis, estando no entanto atenta a todas as discussões a nível internacional (Giles, 2012, p.79). A estratégia que a RU apresenta é essencialmente defensiva e baseia-se em seis princípios: legalidade, prioridade, complexidade, interação, cooperação e inovação. A RU segue as normas do direito internacional mas no domínio informacional uma intervenção externa terá que ser aprovada pelo Presidente, sob proposta do Conselho da Federação da Assembleia Federal. Para a RU, a recolha de informação sobre ameaças é uma prioridade, deixando entender que se sobrepõe à privacidade dos dados. Serão utilizados todos os meios disponíveis para resolver as tarefas que enfrenta, desde tecnologia de ponta a pessoal altamente qualificado. Existe uma interação interministerial, e uma cooperação entre estados amigos e organizações internacionais, tais como a Organização do Tratado de Segurança Coletiva[6](OTSC) ou a Organização para a Cooperação de Xangai. (Russian Armed Forces, 2011, pp.6-8).

No entanto, é sem ilusões que se sabe que a RU tem tido uma postura não oficial, menos defensiva, como foi possível verificar nos ataques à Estónia em 2007 e na guerra com a Geórgia em agosto de 2008 (Robinson et al., 2013). Pode atuar de forma encoberta, apoiando financeiramente grupos como os *Nashi*. Se a RU é vista como uma das nações mais capazes no ciberespaço, Jeffrey Car[7] considera ser a maior ciberameaça para os EUA porque "contrariamente à China, as suas ciberoperações são raramente descobertas" (Carr, 2011).

[6] OTSC ou Tratado de Tashkent é uma aliança militar formalmente assinada em 2002 entre a Arménia, Bielorrússia, Cazaquistão, Quirguistão, Tadjiquistão, Uzbequistão (2006) e a Rússia (ODKB, n.d.)
[7] Jeffrey Carr - Especialista internacionalmente reconhecido em cibersegurança e fundador da *Taia Global*

(2) As entidades responsáveis

O Conselho de Segurança da Federação, presidido pelo Presidente, elabora decisões relativas à segurança e aos interesses vitais das pessoas, da sociedade e do estado . O Ministério para a Defesa Civil, é responsável pelo sistema nacional de proteção da informação. Toda a comunidade dos Serviços de Informações, nomeadamente o Centro de Licenciamento, Certificação e Proteção dos Segredos de Estado dos Serviços de Segurança Federais (FSB) tem um papel ativo na cibersegurança (ODKB, n.d.) (Robinson et al., 2013).

A RU carateriza-se também por utilizar de forma não oficial mas efusiva, grupos de jovens como os *Nashi*, e sindicatos criminosos como o *Russian Business Network* (Smith, 2012, p.3).

(3) Contributo das Forças Armadas

O Ministério da Defesa controla os sistemas que certificam as ferramentas de proteção da informação (Robinson et al., 2013). O ministro da Defesa, Sergei Shoigu ordenou a criação de um "Ciber comando" até ao final de 2013, deixando claro que não pretende "um serviço burocrático com muitos direitos e nenhumas obrigações" a fim de proteger as estruturas de informação da RU (Benitez, 2013). A RU foi capaz de desenvolver uma estrutura de Guerra da Informação, tanto civil como militar, que utiliza de forma eficiente contra os seus adversários. Recentemente, foi identificada uma unidade militar, VCH 71330, disfarçada como a 16ª Divisão dos Serviços de Segurança Federal, responsável pela interceção, desencriptação e processamento de comunicações (Carr, 2011).

d. República Popular da China

(1) A estratégia implementada

A República Popular da China (RPC) é um país tradicionalmente fechado, ficando dificultada a tarefa de pesquisa de fontes primárias próximas da esfera do poder de Pequim. Existem alguns documentos que evidenciam a vontade da RPC em, por exemplo, modernizar as suas FFAA para obter uma vantagem em circunstâncias altamente tecnológicas, nas "cinco dimensões da guerra", associada ao desenvolvimento de nova doutrina e estratégia "*junshi zhidao sixiang*", na era informacional (Huang, 2001, p.140). Uma das referências bibliográficas é a obra de Liang e Xiangsui, *Unrestricted Warfare*, que serviu de inspiração na década de 2000 para o desenvolvimento de capacidades, incluindo as cibernéticas, para conduzir a guerra com países militarmente superiores. As tecnologias de informação são utilizadas para obter ou negar informação (Liang &

Xiangsui, 1999, p.18). Dos oito princípios elencados na obra, realça-se o da "assimetria", que consiste no "rato brincar com o gato" como forma de vencer um adversário mais forte (Liang & Xiangsui, 1999, p.211).

No âmbito civil, a RPC emanou uma estratégia nacional de cibersegurança conhecido como "Documento 27" que aprovou políticas e medidas, de entre elas destacam-se as seguintes: "um esquema de proteção multinível, certificados chineses obrigatórios, recuperação de desastres, gestão de incidentes, segurança governamental, normas de segurança e um plano de segurança da informação a cinco anos" (Lindsay, 2012, p.6).

A RPC tem investido fortemente no seu "12º plano a cinco anos[8]" em capacidades de combate em rede para diminuir o fosso tecnológico que existe, segundo o Coronel Dai Xu, com a Rússia e os Estados-Unidos. A RPC sente-se alvo de ataques como mais ninguém no mundo e, por isto, deseja proteger-se, endurecendo o enquadramento penal para os que cometem ciberataques e cooperando a nível interno com o setor privado e no plano externo com outros países (Lam, 2010).

(2) As entidades responsáveis

Existem quatro agências que fazem a gestão da segurança da informação. O Ministério da Segurança Pública é responsável pelo cibercrime e a proteção das infraestruturas críticas e possui centenas de laboratórios espalhados pelo país. O Serviço de Segurança do Estado preocupa-se com a Segurança da Informação e é o departamento tecnicamente mais capaz e igualmente o mais discreto. A responsabilidade da segurança das telecomunicações e da Internet recai sobre o Ministério da Indústria e das Tecnologias da Informação (MIIT) (Lindsay, 2012)

O Centro Coordenador da Equipa Técnica de Resposta de Emergência Nacional de Redes de Computadores (CNCERT) foi fundado em 1999 e é um dos órgãos do MIIT. Dedica-se a monitorizar, avisar, dar uma resposta de emergência e avaliar a segurança das redes (CNCERT, 2009).

(3) Contributos das Forças Armadas

Em maio de 2011, o porta voz do ministro da Defesa anunciou a criação de um "Exército Azul *online*" como capacidade de ciberdefesa da RPC e a fim de assegurar a segurança da rede militar (ECNS, 2012).

Mark Stokes acredita que o Terceiro Departamento do Estado-maior General do Exército de Libertação Popular serve como "uma autoridade executiva nacional para a exploração de redes de computadores". Tem um papel importante na segurança da informação

[8] série de iniciativas de desenvolvimento econômico-social para os anos 2011-15

de organizações civis e organismos ministeriais. A capacidade ofensiva responsável pelos ataques de computadores em rede (*Computer Network Attack* - CNA) é desconhecida mas Stokes especula que possa existir dentro do Quarto Departamento ou na Segunda Força de Artilharia. Outro autor, Robert Sheldon, encontrou provas da existência de "ciber milícias" constituídas por peritos civis contratados para fins militares (Lam, 2010, pp.22-24).

e. O Reino Unido

(1) A estratégia implementada

O UK definiu em novembro de 2011 uma Estratégia de Cibersegurança centrada em quatro objetivos (Cabinet Office UK, 2011, p.8):

- ✓ Combater o cibercrime e tornar o UK um dos lugares mais seguros do mundo para se fazer negócios;
- ✓ Tornar o UK mais resistente a ciberataques e mais capaz de proteger os seus interesses no ciberespaço;
- ✓ Ajudar a moldar um ciberespaço aberto, vibrante e estável que o público do UK possa usar de forma segura e que suporta as sociedades abertas;
- ✓ Construção do conhecimento de um UK transversal, com aptidões e capacidade para apoiar todos os objetivos de segurança cibernética (Cabinet Office UK, 2011, p.8)

Cada objetivo é esmiuçado em objetivos específicos cuja responsabilidade é atribuída a um determinado Ministério.

O UK implementou, para um período de quatro anos, um programa ambicioso de cibersegurança que recebeu 755 milhões de euros (Cabinet Office UK, 2011, p.8). Na consecução dos objetivos definidos, o governo não tem a pretensão de contrariar de *per si* as ameaças, que são catalogadas em quatro tipos: criminosos, atores estatais, terroristas e *hacktivistas*. Estas podem ser transnacionais, necessitando do apoio de outros parceiros e, mesmo a nível interno, grande parte das infraestruturas de comunicação pertence a privados. Neste sentido, a abordagem é holística e estende-se ao "setor privado, indivíduos e ao governo que devem trabalhar em conjunto" (Cabinet Office UK, 2011, p.22).

(2) As entidades responsáveis

A organização das entidades responsáveis pela cibersegurança do UK é relativamente simples (Anexo E).

(a) Conselho Nacional de Segurança

O Conselho Nacional de Segurança (*National Security Council*) é um fórum de discussão da segurança nacional que procura tornar homogénea e transversal a estratégia interministerial para a segurança nacional. Reúne-se semanalmente e é liderado pelo Primeiro Ministro (Cabinet Office, 2012).

Em Outubro de 2010, elaborou a Estratégia Nacional de Segurança, "Um Reino Unido forte numa era de incerteza". O UK classifica os ciberataques no grupo de topo dos quatro maiores riscos, ao mesmo nível que os ataques do terrorismo internacional, o que evidencia bem a importância que lhe é atribuída (Government, 2010, p.11).

(b) *Cabinet Office*

O Gabinete para a Cibersegurança e a Segurança da Informação (*Office for Cyber Security and Information Assurance* - OCSIA) coordena as atividades de cibersegurança de forma transversal no governo e gere o programa nacional de cibersegurança (*National Cyber Security Programme* - NCSP) (House of Commons Defence Committee, 2013, p.39)

(3) Contributo das Forças Armadas

O Ministério da Defesa (UK MoD) recebe 14% do orçamento do NCSP para integrar as questões cibernéticas na Defesa (Cabinet Office UK, 2011, p.25), assegurando que as redes militares e os diversos equipamentos são protegidos contra os ciberataques. O Comando de Forças Conjunto (*Joint Forces Command* - JFC) que entrou em funcionamento em Abril 2012, irá lidar o desenvolvimento e integração das capacidades de ciberdefesa (Cabinet Office UK, 2011, p.26).

O UK MoD contribuiu para a elaboração da estratégia nacional de cibersegurança e mantém uma relação próxima do OCSIA o que facilita a produção de novas políticas na mesma linha de pensamento e no mesmo espírito do que os restantes ministérios. Contudo, não lhe cabe a responsabilidade de proteção das Infraestruturas Críticas Nacionais, sendo esta do Centro para a Proteção das Infraestruturas Nacionais (CPNI) (UK Parliament, 2012).

Em relação ao objetivo dois "tornar o UK mais resistente a ciberataques e mais capaz de proteger os seus interesses no ciberespaço", o UK MoD é responsável pelo objetivo específico "assegurar que o RU é capaz de proteger os seus interesses no ciberespaço melhorando a capacidade de detetar as ciberameaças e aumentando a capacidade de dissuasão e impedir ataques" (UK Parliament, 2012)

(a) Grupo de Operações de Ciberdefesa

O *Defence Cyber Operations Group* (DCOG) irá pertencer ao Comando de Forças Conjuntas e deverá estar totalmente operacional em março de 2015, concentrando numa única estrutura os peritos cibernéticos. É uma capacidade de ciberdefesa composta por uma federação de unidades cibernéticas que trabalham em conjunto, sendo responsável pela cibercultura a desenvolver transversalmente no MoD; pelo planeamento coerente das ciberoperações; assegurar que os comandantes sejam conhecedores do impacto do ciberespaço nas operações e ser ainda capaz de conduzir ciberoperações (House of Commons Defence Committee, 2013, p.21).

Para 2015, está prevista a criação na dependência do DCOG de mais uma Ciberunidade Conjunta (*Joint Cyber Unit*), para desenvolver "novas táticas, técnicas e planos a fim de atingir efeitos militares nas ciberoperações" (House of Commons Defence Committee, 2013, p.22).

(b) Quartel General das Comunicações do Governo (GCHQ)

É uma das três agencias de informações do país, juntamente com o MI5 e o MI6. As suas raízes surgiram há mais de um século, e a sigla nasceu inicialmente em 1939, como uma designação encoberta da *Government Code and Cyber School*. Neste sentido, é possível ler-se na página inicial do site do Quartel General das Comunicações do Governo (GCHQ) a seguinte frase: "o GCHQ providencia informações, protege e informa a política relevante do Reino Unido para manter a nossa sociedade segura e bem sucedida na era da Internet" (GCHQ, 2013).

O GCHQ recebe 59% do orçamento do NCSP (Cabinet Office UK, 2011, p.25).

No seio do GCHQ, existe um Centro de Operações de Cibersegurança (*Cyber Security Operations Centre* - CSOC) que monitoriza e prioriza os incidentes, assegurando que o governo só tem uma única versão dos factos para ação (House of Commons Defence Committee, 2013, p.42).

O UK colabora com os EUA e a Austrália através de um memorando de entendimento trilateral, mantém ainda acordos de cooperação na defesa onde está prevista a vertente cibernética, com a França e participa no NATO *Incident Response and Command Centre* sediado na Bélgica (House of Commons Defence Committee, 2013, p.28). O UK identificou algumas dificuldades no recrutamento e na retenção de peritos na área da cibersegurança. Existe uma elevada rotação do pessoal militar e são numerosas as saídas do setor público para o privado, financeiramente mais atrativo (House of Commons Defence Committee, 2013, p.22).

f. Tabela recapitulativa da resposta dos países

Tabela 4 - Exemplos de estratégias de cibersegurança

Fonte: (Robinson et al., 2013)

PAÍS	ESTRATÉGIA (S,N)/ PRIORIDADE DAS CIBERAMEAÇAS	ENTIDADE PRINCIPAL RESPONSÁVEL / ENTIDADE MILITAR
EUA	Sim (2010) / máxima	*National Cyber Security Center do Department of Homeland Security,* USCYBERCOM do USSTRATCOM
NL	Sim (2011) / elevada	*National Cyber Security Centre,* *Cyber Taskforce* do Ministério da Defesa
RU	Sim (2009)	*Security Council of the Federation,* Ministério da Defesa, VCH 71330
RPC	Sim	Ministério da Segurança Pública Serviço de Segurança do Estado MIIT Exército Azul *online*
UK	Sim (2009) / máxima	*Office of Cyber Security and Information Assurance,* *Cyber Security Operations Centre*
Rússia	Sim	*Security Council of the Federation,* Ministério da Defesa

3. Organizações Internacionais

"Amai a união e fugi das discórdias"

Santo Inácio de Antioquia (35 – 107)

As ameaças cibernéticas, que não conhecem fronteiras e cuja fonte é por vezes difícil de detetar, podem precisar de uma resposta que transcende a capacidade de um único estado, por mais poderoso que seja neste domínio. Neste capítulo, é abordada a visão de algumas organizações em relação à cibersegurança e tentaremos assinalar quais as oportunidades que Portugal pode retirar de uma cooperação no seio das alianças.

a. Organização do Tratado do Atlântico Norte

(1) A estratégia implementada

A Organização do Tratado do Atlântico Norte (NATO) começou por constatar as suas vulnerabilidades no ciberespaço após o bombardeamento da embaixada chinesa durante a intervenção nos Balcãs em 1999 que teve por consequência uma avalanche de ataques aos *web sites* da coligação. Mais recentemente, a NATO voltou a admitir fragilidades na sequência do ataque de negação de serviços distribuída (*Distributed Denial of Service* – DDOS) sofrido pela Estónia em 2007, que deixou este país paralisado por três semanas. Na cimeira de Lisboa em novembro 2010, foi aprovado o "novo conceito estratégico da NATO, compromisso ativo, defesa moderna", no qual a organização se compromete a desenvolver capacidades para "prevenir, detetar, defender e recuperar de ciberataques (...) coordenando as capacidades de ciberdefesa nacionais (...)". Nesse documento são reconhecidas as seguinte ameaças: serviços de informações e militares estrangeiros, crime organizado, grupos terroristas e extremistas (NATO, 2010). O processo de planeamento da NATO, comum, padronizado e aceite pelos membros da organização pode ser um dos instrumentos facilitadores da coordenação das capacidades de ciberdefesa dos aliados.

Em 2011, é assinada uma revisão da "política da NATO para a ciberdefesa". O objetivo principal é garantir a proteção dos sistemas de comunicações e de informação da NATO e são tomadas as seguinte medidas: integração da ciberdefesa nas estruturas de defesa nacionais através do Processo de Planeamento de Defesa da NATO; desenvolvimento de requisitos mínimos para as redes dos países que se ligam com, ou tratam informação da Organização; seguir os princípios da prevenção, resiliência e não duplicação; coordenar a ajuda em caso de ciberataque; cooperar com outros parceiros, organizações internacionais, as universidades e o setor privado (NATO, 2011).

Portugal, como membro fundador, não deveria ser o elo mais fraco da organização e uma porta de entrada para *malware*, sobre pena de perder credibilidade e correr o risco de não ser considerado de confiança em operações militares combinadas futuras, por não possuir a grau de proteção adequado nas suas FFAA. Assim, Portugal é obrigado a manter umas FFAA prontas, bem equipadas e capazes de acompanhar os seus parceiros na defesa coletiva.

A NATO caminha para o desenvolvimento de capacidades defensivas conhecido por "*Forces 2020"* que tem por objetivo: "desenvolver forças modernas, equipadas e interligadas, treinadas e comandadas de forma a operarem em conjunto e com outros parceiros em qualquer ambiente" (NATO, 2012). Este novo percurso da NATO esta estreitamente ligado a dois conceitos atualmente populares, associados à *Comprehensive Approach*[9]. Por um lado, a *Connected Forces Initiative*[10] (CFI) que consiste em manter a prontidão, eficiência e interoperabilidade da NATO através de uma maior formação e treino, um aumento do número de exercícios e um acréscimo da utilização da tecnologia (Kohl, 2013). Por outro lado, ciente das dificuldades económicas atuais, a NATO procura desenvolver, no quadro do novo conceito estratégico, um caminho que leve à cooperação, ao desenvolvimento, aquisição e manutenção de capacidades militares em conjunto: "*Smart defence"* (NATO, 2012). Como referiu o General Quesada Pastor, a *Smart Defence* visa dotar a aliança com as capacidades necessárias para o seu nível de ambição, enquanto que a CFI pretende dotar a aliança das capacidades de efetuar todo o espetro de missões após 2014, onde se incluem, as ciberoperações (Pastor, 2013). Em 14 de março de 2013, cinco países[11] lançaram o "projeto multinacional de desenvolvimento de capacidades de ciberdefesa" enquadrado nas iniciativas de *Smart Defence* (NATO, 2013). Este projeto pertence ao *Tier um,* ou seja, onde se inserem os programas de maior comprometimento das nações.

A NATO enfrenta alguns dilemas relacionados com a ação coletiva: os ciberataques podem não afetar todos os países da mesma forma o que poderá se traduzir em graus de solidariedade diferentes; as ciberameaças não são vistas necessariamente como ameaças militares a não ser que sejam consideradas juridicamente como tal; os ciberataques podem ter uma resposta que não seja unicamente militar. Estes dilemas são atenuados se existir uma mudança de mentalidades, passando-se de ações de dissuasão

[9] abordagem global
[10] CFI – Iniciativa de Forces Ligadas
[11] Canada, Dinamarca, Holanda, Noruega e Roménia.

para a prevenção, resiliência, gestão das consequências e o desenvolvimento de capacidades para o ciberespaço (Ruhle, 2013).

(2) Entidades responsáveis

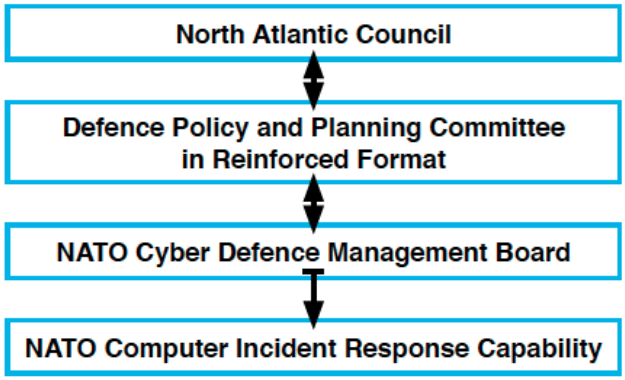


Figura 1 - Organização da ciberdefesa na NATO

Fonte: (NATO, 2011)

O *North Atlantic Council*[12] (NAC) supervisiona todos os aspetos da implementação das políticas de ciberdefesa, ao mais alto nível. O *Defence Policy and Planning Committee*[13] (DPPC) aconselha a aliança sobre os esforços de ciberdefesa. O *NATO Cyber Defence Management Board*[14] (CDMB) é responsável por coordenar a ciberdefesa entre os organismos civis e militares da Organização, e trabalha sob a dependência da *Emerging Security Challenges Division*[15] (ESCD). A implementação e aconselhamento técnico são assegurados pela NATO *Consultation, Control and Command Board*[16] (NC3B). A NATO *Computer Incident Response Capability* (NCIRC) foi criada em fevereiro 2012 com um orçamento de 58 milhões de euros, pertence à recente *NATO's Communications and Information Agency*[17] (NCIA) e proporciona serviços de cibersegurança técnica e operacional dentro da NATO. Atinge a capacidade operacional plena (*Full Operational Capability* - FOC) em 2013, e todos os Centros de Dados da NATO terão capacidades de ciberdefesa defensivas e ofensivas (NCIA COS, 2013). Existe ainda uma *Cyber Threat Awareness Cell*[18] com a missão de aumentar a partilha de informações e o conhecimento da situação e um Centro de Excelência, o *Cooperative Cyber Defence Centre of Excellence* (CCDCoE), na Estónia, que desde 2008, investiga e treina na área da ciberdefesa (NATO, 2013).

[12] NAC - Conselho do Atlântico Norte (tradução do autor)
[13] DPPC - Comité de Planeamento e de Política de Defesa (tradução do autor)
[14] CDMB - Conselho de Gestão de Ciberdefesa (tradução do autor)
[15] ESCD – Divisão dos Desafios Emergentes de Segurança (tradução do autor)
[16] NC3B – Bordo de Aconselhamento, Comando e Controlo da NATO (tradução do autor)
[17] NCIA – Agência de Comunicações e de Informação da NATO (tradução do autor)
[18] Célula de Conhecimento da Ciberameaça

b. União Europeia

(1) A estratégia implementada

Em termos históricos, a Comissão Europeia tem-se vindo a debruçar sobre a importância da Segurança da Informação e das Redes a partir de 2001, numa primeira "proposta de uma política europeia". Em 2006, adotou uma "estratégia para uma sociedade da informação segura", visando desenvolver uma cultura de segurança da informação. Em 2009 difundiu um comunicado sobre a proteção das infraestruturas críticas de informação, " Proteger a Europa de ciberataques em grande escala e disrupções: aumentar a preparação, segurança e resiliência", que deu origem a uma resolução do conselho, "uma abordagem europeia colaborativa à segurança da informação e das redes". Em maio de 2010, a "Agenda Digital para a Europa" (DAE) realçou a necessidade de prevenção, preparação, conhecimento e o desenvolvimento e coordenação de mecanismos de segurança, que seriam a base da proposta de estratégia de fevereiro de 2013 (Comissão Europeia, 2013).

A visão da União Europeia (UE) para o ciberespaço traduz-se numa estratégia constituída por cinco prioridades (Comissão Europeia, 2013):

"

- ✓ alcançar uma ciber resiliência;
- ✓ Reduzir drasticamente o cibercrime;
- ✓ Desenvolver uma política de ciberdefesa e capacidades relacionadas com a Política Comum de Segurança e Defesa (PCSD);
- ✓ Desenvolver recursos tecnológicos e industriais para a cibersegurança;
- ✓ Estabelecer uma política internacional coerente no ciberespaço para a UE e promover valores nucleares da UE."

(2) As entidades responsáveis

A figura abaixo sublinha a importância da interligação entre as várias entidades, representada graficamente pelas setas nos três vetores: segurança das redes e da informação, cumprimento da lei e Defesa. Realça igualmente a importância da cooperação internacional com a ligação aos estados-membros. Finalmente, o papel da indústria e do ensino é transversal e necessário em todo o processo.

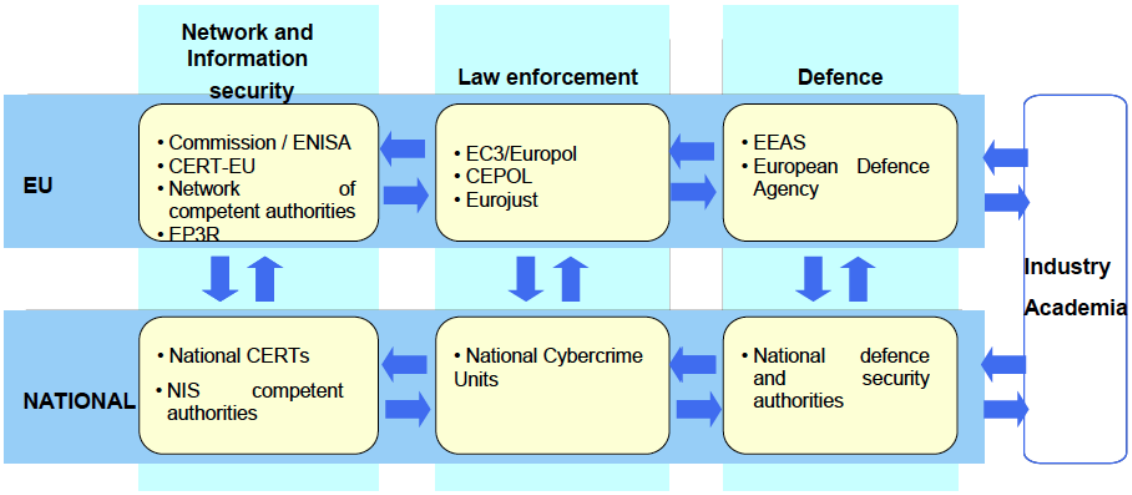


Figura 2 - Entidades responsáveis pela cibersegurança na UE

Fonte: (Comissão Europeia, 2013)

(a) ENISA

A Agencia Europeia de Segurança da Informação e das Redes (*European Network and Information Security Agency* - ENISA) foi criada em 2004 e tem como tarefas principais o aconselhamento, a análise de dados, o aumento do conhecimento e a cooperação entre as agencias da UE e os estados membros (ENISA, 2013).

(b) CERT-EU

A Equipa de Resposta de Emergência de Computadores da UE (*Computer Emergency Response Team* – CERT-EU) foi criada em setembro de 2012. É constituída por especialistas em segurança das Tecnologias da Informação das principais Instituições da UE e coopera com os CERTs nacionais e empresas especializadas na segurança. Tem por missão a ajuda às instituições europeias na proteção contra ciberataques (CERT-EU, 2013).

(c) Europol/EC3

O Centro de Cibercrime Europeu (*European Cybercrime Centre* – EC3) foi criado em janeiro de 2013, como uma estrutura da *European Police Office* (EUROPOL) e é a entidade principal de luta contra o cibercrime na Europa.

(3) O setor da defesa europeia

A Agência Europeia de Defesa (*European Defence Agency* - AED), sediada em Bruxelas, foi criada em julho de 2004 e é constituída por 26 Estados-membros, incluindo Portugal. Tem por missão "suportar o Conselho e os Estados-membros no esforço de melhorar as capacidades de defesa da UE para a PCSD" (European Defence Agency,

2012). Os seus objetivos principais na área da defesa são a cooperação dentro da UE no domínio do armamento, o reforço da base tecnológica e industrial, a criação de um mercado europeu competitivo dos equipamentos e a promoção da investigação (União Europeia, 2012). A AED participou na elaboração da estratégia de cibersegurança da EU. Encontra-se atualmente a desenvolver capacidades de ciberdefesa e tecnologias, melhorar o treino e a condução de exercícios. Um dos maiores exercícios conduzidos neste domínio a nível mundial foi o "*Cyber Europe* 2012", que contou com a participação de 25 países, incluindo organizações portuguesas (ENISA, 2012).

A cooperação é hoje fundamental e, num cenário de crise económica onde algumas capacidades militares podem desaparecer ou nem sequer ser geradas deve ser ainda mais potenciada. Neste sentido, devem-se efetivamente procurar sinergias dentro dos parceiros da UE, uma maior cooperação na investigação, nos custos de desenvolvimento, uma partilha na aquisição de equipamentos críticos e, eventualmente, a especialização de alguns estados numa determinada área, algo que pode ser ainda visto como controverso. Um dos novos conceitos em voga é o de *Pooling and Sharing*, necessário para a afirmação em conjunto dos países da UE num mundo global onde o domínio americano no setor da defesa vê o aparecimento de atores emergentes, cada vez mais fortes. A chave do sucesso reside na "ligação e complementaridade" de programas com os da NATO, e um processo de despolitização, cujas agendas normalmente têm um horizonte temporal de uma legislatura, incompatível com a manutenção de programas com horizontes temporais alargados (Faleg & Giovannini, 2012).

No quadro da UE, Portugal tem o "maior interesse estratégico na estabilidade, coesão e aprofundamento do projeto europeu" e por isso, tem participado em missões de Petersberg e contribui com capacidades militares, no esforço comum (Conselho de Ministros 6/2003, 2003, p.285). A política europeia de segurança e defesa foi, no Tratado de Lisboa, substituída pela PCSD, que visa atingir uma defesa europeia comum. O principal instrumento da PCSD é a AED que procura agregar objetivos comuns, criando programas para ir ao encontro das necessidades operacionais, fomentar a investigação tecnológica e a indústria de defesa (Europa, 2010).

c. Organização das Nações Unidas

A Organização das Nações Unidas (ONU) tem mantido atividades desde 2003 relacionadas com a cibersegurança em geral e a cibercriminalidade em particular. Após algumas iniciativas infrutíferas para alcançar um consenso alargado, foi finalmente elaborado um relatório em 2010 que recomendava "um diálogo entre os estados na

discussão de normas relativas à utilização das Tecnologias de Informação e Comunicação (TIC), para reduzir o risco coletivo e proteger as infraestruturas críticas nacionais e internacionais" (UNODA, 2010). As principais divergências no seio da ONU centram-se numa corrente de pensamento que procura o desenvolvimento de capacidades de cibersegurança e outra oposta, que pretende o desenvolvimento de legislação. (OECD, 2012, p.39). Contrastando com todas as atividades mal intencionadas atribuídas habitualmente à RU e à RPC, frequentemente noticiadas, estas nações têm sido particularmente dinâmicas na ONU, considerando-se vítimas de ciberataques e por isso, realçam a necessidade de cooperação, o desenvolvimento de normas e princípios internacionais de responsabilização (ONU, 2011). A Assembleia Geral da ONU adotou várias resoluções, destacando-se a 57/239 "*Creation of a global culture of cybersecurity*[19]" (OECD, 2012, p.39).

No seio da ONU, existe uma agência especializada nas TIC, a *International Telecommunication Union*, que trabalha em três áreas principais: comunicações rádio, elaboração de normas e desenvolvimento do setor de telecomunicações (ITU, 2013). Para os países que ainda não elaboraram uma estratégia ou estão num processo de revisão, a ITU emanou um conjunto de recomendações que podem servir de guia. Os dez elementos identificados para o desenvolvimento de um programa nacional de cibersegurança são os seguintes: responsabilidade de cibersegurança ao mais alto nível governamental; um gabinete coordenador da atividade de cibersegurança a nível nacional; um organismo único agregador de várias valências como ponto central para a cibersegurança nacional; Enquadramento legal adequado às novas ameaças; *Computer Incident Response Teams* (CIRT) para acompanhar a evolução das ameaças e fazer a gestão dos incidentes; consciencialização e educação dos vários setores da sociedade; parcerias entre o setor público e privado; programas de treino e desenvolvimento de capacidades para profissionais; cooperação internacional para enfrentar ameaças transnacionais (Wamala, 2011, p.6).

[19] Criação de uma cultura global de cibersegurança – tradução do autor

4. O caso nacional

"O país não precisa de quem diga o que está errado; precisa de quem saiba o que está certo."
Agustina Bessa-Luís (1922 - ...)

a. A estratégia de cibersegurança nacional

Ainda não se desenvolveu nenhuma verdadeira ciberestratégia em Portugal mas a maioria dos nossos parceiros da NATO e na Europa já sentiram recentemente esta necessidade. As iniciativas individuais, incoerentes em termos globais deverão ser evitadas a fim de reduzir a duplicação de atividades e a má utilização dos escassos recursos disponíveis. Sem estar devidamente precavido, um cenário análogo ao vivido na Estónia teria consequências semelhantes em Portugal. Por isso, Portugal terá que criar a sua estratégia, porque é um país dependente do ciberespaço, com uma economia baseada essencialmente no comércio e serviços. Vamos agora passar à análise do ponto de situação nacional.

Em 2005, podemos considerar que Portugal estava "na vanguarda na Europa e na NATO para a criação de uma Estratégia Nacional da Segurança da Informação (ENSI)" mas atualmente, é um dos países mais atrasados (Honorato, 2012). A ENSI em vigor é ainda atual, precisando de uma revisão a fim de ser adaptada à nova situação. Hierarquicamente dependente da ENSI, pode ser desenvolvida uma Estratégia Nacional de Cibersegurança (ENC). Viegas Nunes, reconhecido perito nacional em cibersegurança, propõe o levantamento de uma ENC, enquadrada na Estratégia de Segurança e Defesa do Estado que é parte da Estratégia da Informação Nacional, e define três objetivos: garantir a segurança do ciberespaço; melhorar a eficiência da utilização da informação e explorar o ciberespaço com eficácia. Desenvolve "linhas de ação estratégica" que iremos apresentar sucintamente: garantir a proteção das Infraestruturas de Informação Críticas, melhorar a segurança das TIC nacionais, rever a moldura legal, levantar novas estruturas como o Conselho Nacional de Cibersegurança e Ciberdefesa, o Centro Nacional de Cibersegurança, desenvolver iniciativas nacionais e reforçar a cooperação internacional (Nunes, 2012, pp.122-24). O Gabinete Nacional de Segurança (GNS) elaborou uma proposta de Estratégia Nacional de Cibersegurança centrada em três objetivos: "garantir a segurança no ciberespaço; fortalecer a cibersegurança das infraestruturas críticas nacionais; defender os interesses nacionais e a liberdade de ação no ciberespaço" (GNS, n.d.). Em

resumo, podemos concluir que as linhas de ação estratégica não diferem muito daquelas elencadas por Viegas Nunes.

O novo Conceito Estratégico de Defesa Nacional (CEDN) aprovado em Conselhos de Ministros em 21 de Março de 2013, substitui o anterior de 2003. Apresenta vetores e linhas de ação para adequar as políticas de segurança e defesa nacional ao ambiente estratégico e, em resposta às ameaças e riscos no domínio da cibercriminalidade, propõe que seja feita uma avaliação das vulnerabilidades e define cinco linhas de ação: "garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN); definir uma Estratégia Nacional de Cibersegurança; montar a estrutura responsável pela cibersegurança, através da criação dos órgãos técnicos necessários; sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática; e levantar a capacidade de ciberdefesa nacional" (RCM, 2013a, p.35). No seguimento da divulgação do CEDN, deverá ser fechado o ciclo de planeamento estratégico nacional: a elaboração de estratégias particulares tais como a ENSI e a ENC; um novo conceito estratégico militar, do qual decorrera uma atualização das missões das FFAA.

b. A abordagem das ciberameaças em Portugal

É interessante, como ponto de partida da argumentação, analisar a relação entre a ciberdefesa e a cibersegurança juntamente com os atores que detêm responsabilidades.

Tabela 5 - Tipologia das ciberameaças

Fonte: (Nunes, 2012)

TIPOLOGIA	AMEAÇA	ENTIDADE RESPONSÁVEL
CIBERSEGURANÇA	Cibercrime	Forças de Segurança
	Hacktivismo	
	Ciberespionagem	Serviços de Informação
	Ciberterrorismo	
CIBERDEFESA	Ciberguerra	Forças Armadas

Observa-se na tabela acima que tanto o cibercrime como o *hacktivismo* são da responsabilidade das FFSS. A Polícia Judiciária tem a competência reservada da investigação dos crimes informáticos e os praticados com recurso a tecnologia informática (Assembleia da República, 2008) e exerce esta competência por intermédio da Unidade Nacional de Combate à Corrupção (PJ, 2013).

Em relação ao ciberespionagem e cibeterrorismo, são tipologias da responsabilidade dos Serviços de Informação. O Diretor Geral do Serviço de Informações de Segurança (SIS), juiz desembargador Laço Pereira Pinto refere que a capacidade atual de cibersegurança dos Serviços de Informações da República Portuguesa (SIRP), ainda embrionária, encontra-se num departamento comum ao Serviço de Informações Estratégicas de Defesa (SIED) e do SIS (Pinto, 2013). A Lei de Segurança Interna consagra no Artigo 35º que "as FFAA colaboram em matéria de segurança interna nos termos da Constituição e da lei, competindo ao Secretário-Geral do Sistema de Segurança Interna (SGSSI) e ao Chefe do Estado-Maior-General das FFAA (CEMGFA) assegurarem entre si a articulação operacional" (Assembleia da República, 2008). Conclui-se que existe espaço para um contributo das FFAA num espetro mais alargado do que a ciberdefesa, podendo, dentro da lei, colaborar com as FFSS e os Serviços de Informação. Todavia, esta articulação merece um maior desenvolvimento, sendo necessário definir com precisão o seu alcance. Na opinião do SGSSI, o juiz desembargador Antero Luís, a Constituição da República Portuguesa (CRP) é pouco precisa no seu Artigo 275º, no que diz respeito à possível colaboração das FFAA com as FFSS, nomeadamente entre os estados de exceção e o estado normal, onde existe uma zona de sombra, passível de ser resolvida por duas vias: alteração da constituição sem distinção entre a segurança interna e a segurança externa; emanação de uma Resolução do Conselho de Ministros clarificadora e densa sobra a articulação entre FFSS e as FFAA (Luís, 2013). O mesmo autor defende que um único Centro de Cibersegurança não é suficiente, sendo necessários três centros diferentes: um para o cibercrime, outro para a ciberdefesa e outro para os serviços de informações.

Relativamente ainda às ameaças, visualiza-se uma pequena evolução contrastando com o relatório da ENISA que afirmava que Portugal não tinha uma lista consolidada. O novo CEDN reconhece que o "processo de globalização e a revolução tecnológica tornaram possível (...) uma difusão equivalente de ameaças e riscos em todas as dimensões (...) e o potencial devastador dos ataques cibernéticos" (RCM, 2013a, p.8) e que estas ameaças são "o ciberterrorismo e a cibercriminalidade, tendo por alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada" (RCM, 2013a, p.14) Concretiza ao afirmar que "os ciberataques são uma ameaça crescente a infraestruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização moderna" (RCM, 2013a, p.15; RCM, 2013b)

Quando este patamar estiver à beira de ser atingido, Portugal tem que dispor de

capacidades suficientes para se proteger e eventualmente, contra atacar. Nas "Linhas gerais da reforma da defesa 2020", o ministro da Defesa refere precisamente a necessidade de prever "o levantamento da capacidade de ciberdefesa nacional", ao mesmo nível que outras reformas estratégicas das FFAA nos próximos anos, o que revela a importância que a temática tem nos dias de hoje, indicando claramente que Portugal despertou finalmente para a cibersegurança: existem vontade e orientações políticas.

Observemos as estruturas portuguesas capazes de operacionalizar esta estratégia.

c. Entidades responsáveis pela cibersegurança em Portugal

(1) Gabinete Nacional de Segurança

O GNS tem por missão "garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exercer a função de autoridade de credenciação de pessoas e empresas para o acesso e manuseamento de informação classificada, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Electrónica do Estado - Infraestrutura de Chaves Públicas (SCEE)" (GNS, 2012).

(2) Centro Nacional de Cibersegurança

A Resolução do Conselho de Ministros n.º 42/2012 constituiu a Comissão Instaladora do Centro Nacional de Cibersegurança (CNCSeg), na dependência do Primeiro-Ministro (PM) e presidida pela Autoridade Nacional de Segurança. Dos elementos integrantes está um representante do membro do Governo da área da defesa nacional. Foi apresentado um relatório em junho de 2012 que prevê a implementação faseada do CNCSeg até 2015, na dependência direta do PM.

Aguarda-se para muito breve a *Initial Operational Capability* (IOC) do CNCSeg, como uma estrutura inicialmente paralela ao GNS que se deverá independentizar no futuro. Será constituído por onze elementos (Marques, 2013). O CNCSeg será a estrutura principal e agregadora da cibersegurança nacional, interligando-se internamente com as entidades que iremos seguidamente ver, mas igualmente no plano externo com estruturas análogas dos nossos parceiros, da NATO e da UE.

(3) CERT.PT

O Serviço de Resposta a Incidentes de Segurança Informática CERT.PT foi criado em 2000 e acreditado em 2004, sendo o CERT português. Tem como missão "contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal." (CERT.PT, 2013) Promove ações de formação

para vários setores, incluindo as FFAA. Mantém ligações com outros CERTs, a UE através da ENISA e a NATO.

(4) Outras entidades

Tabela 6 - Outras entidades nacionais com responsabilidade de cibersegurança

NOME		MISSÃO
ICP-Anacom	Instituto das Comunicações de Portugal – Autoridade Nacional de Comunicações	Regula e supervisiona o sector das comunicações eletrónicas e postais em Portugal, assegurando a representação nacional nos diversos fora internacionais relevantes (ANACOM, 2011).
UMIC	Agência para a sociedade do conhecimento	Organismo público português com a missão de coordenar as políticas para a sociedade da informação e mobilizá-la através da promoção de atividades de divulgação, qualificação e investigação, promover o desenvolvimento tecnológico e a criação de conhecimento por entidades do sistema científico e tecnológico e por empresas, e estimular o desenvolvimento da e-Ciência (UMIC, 2006).
CNPD	Comissão Nacional de Proteção de Dados	Entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República (Assembleia da República, 2004) Tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei
CERT-IPN	*Computer Security Incident Response Team* (CSIRT)	Integrado no Laboratório de Informática e Sistemas do Instituto Pedro Nunes, uma instituição privada de utilidade pública sem fins lucrativos, que tem como missão a transferência de tecnologia entre a Universidade e o tecido económico Português
CSIRT.FEUP	CSIRT da Faculdade de Engenharia do Porto	"Serviço web para disseminação de alertas de segurança. Possibilita a todos os utilizadores receberem ou consultarem alertas de segurança" (CSIRT.FEUP, 2013).
ANETIE	Associação Nacional das Empresas das Tecnologias de Informação e Eletrónica	"Tem por missão defender os interesses do sector empresarial de Tecnologias de informação e Electrónica e promover o seu crescimento sustentado" (ANETIE, 2012).
APRITEL	Associação dos Operadores de Telecomunicações	"Promove o desenvolvimento de ambiente legal e regulamentar favorável ao investimento no setor das comunicações eletrónicas e contribuir para o desenvolvimento da Sociedade de Informação" (APRITEL, 2013).
FCCN	Fundação para a Computação Científica Nacional	"Disponibiliza meios avançados de comunicações para a comunidade de investigação e de ensino nacional, contribuindo para a dinamização das tecnologias e serviços da Internet em Portugal" (FCCN, 2013)

d. As Forças Armadas portuguesas

As FFAA são responsáveis pela ciberdefesa, nomeadamente através do que era conhecido como as CNO e que foi recentemente revisto pelos EUA na *Joint Publication 3-12* "C*yberspace Operations"* como ciberoperações: utilização de capacidades cibernéticas ofensivas e defensivas que consistem em negar ou manipular um meio informacional, uma mensagem ou uma ciber entidade a fim de alcançar objetivos no ou através do ciberespaço (Joint Chiefs of Staff, 2012, p.II_9). Consideramos que existe algum espaço para as FFAA poderem contribuir com as outras entidades: FFFSS, Serviços de Informação, outros organismos públicos e eventualmente privados.

O esforço de participação das FFAA na cibersegurança pode ser visto em três níveis. A figura abaixo ajuda a perceber os diferentes graus de contribuição das FFAA no decorrer de ciberataques patrocinados, por exemplo, por *hacktivistas*, com níveis de disrupção crescentes em relação à capacidade de resposta das FFSS.

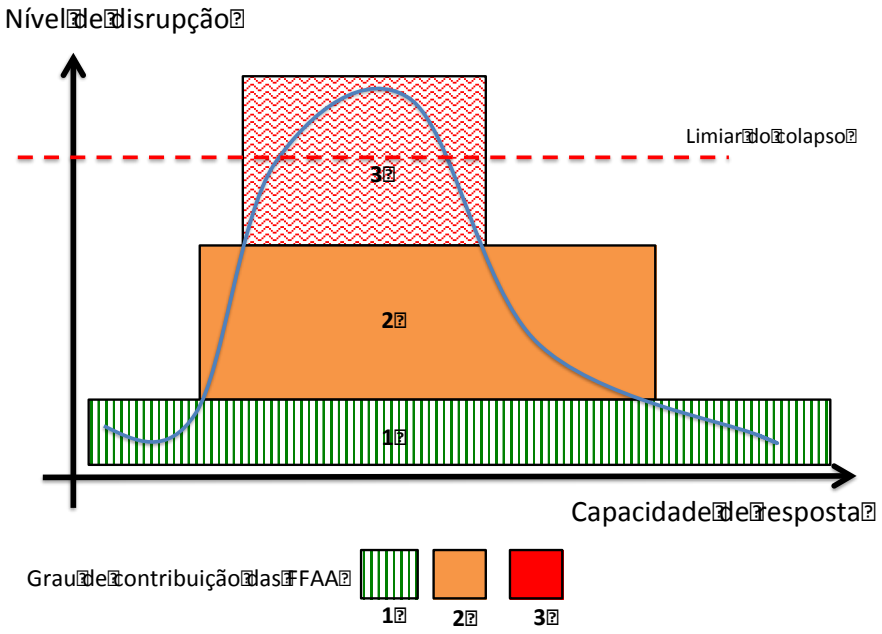


Figura 3 - Os diferentes graus de participação das FFAA na resposta ao escalar de ciberataques

Os graus de contribuição não são estanques. No primeiro nível, "Grau de contribuição um" na figura, vemos as FFAA como um ator participativo no esforço global de cibersegurança, que é uma responsabilidade de todos. Desde o ciberespaço individual criado nas nossas casas e que temos obrigação de manter seguro, passando pelos órgãos responsáveis pelas Infraestruturas Críticas Nacionais, as FFAA contribuem igualmente com a segurança das suas próprias redes (Marques, 2013), que são de vários tipos: uma

infraestrutura física que cobre o território nacional, interligando as várias unidades ou bases no Continente e nas ilhas; uma extensão para os vários teatros de operações, com recurso a ligações de satélite alugadas a operadoras internacionais, uma vez que Portugal não possui esta capacidade; ligações a redes táticas através de Pontos de Interoperabilidade, quando necessário, para efeito operacionais ou de Exercícios.

A rede principal, denominada por Sistema Integrado de Comunicações Militares (SICOM), é administrada pelo Estado Maior General das Forças Armadas (EMGFA). A Capacidade de Resposta a Incidentes de Segurança Informática (CRISI) foi criada em 2008, no EMGFA. É sabido, através de uma Resolução do Conselho de Ministros recente, que a estrutura do EMGFA irá ser adaptada a fim de receber um "único serviço que coordene as comunicações e os sistemas de informação, em articulação com os ramos, procurando-se a sua centralização num único polo e a implementação de uma plataforma transversal de apoio à decisão, designadamente no que diz respeito às funções de comando, controlo e direção. O Centro de Ciberdefesa a criar deverá estar localizado junto deste serviço" (RCM, 2013b).

Os ramos conservam ainda assim poderes de gestão dos utilizadores e máquinas nas suas redes, sendo os responsáveis pela segurança das mesmas. Neste campo, têm desenvolvido esforços independentes.

A Marinha gere o domínio "marinha.pt" e tem tido uma preocupação crescente com a ciberdefesa. Com a extinção dos Centros de Comunicações, alguns dos oficiais, nomeadamente técnicos, foram reciclados com ações de formação na área da ciberdefesa, juntamente com sargentos e civis que podem vir a ser selecionados para estagiar no CERT.PT. A capacidade de ciberdefesa da Marinha é todavia incipiente, consistindo num Centro de Resposta que existe no Centro de Comunicações, de Dados e de Cifra da Marinha (CDCM), que pertence ao Comando Naval. A Marinha tem desenvolvido outras iniciativas e, a título de exemplo, os navios estão equipados com uma ferramenta de análise em tempo real dos alertas de segurança dos equipamentos das redes, o *Security Information and Event Management* (SIEM). No sentido de construir um Conhecimento Situacional Marítimo[20] (CSM), a Marinha vê imperativo o desenvolvimento de uma capacidade de cibersegurança para a comunidade marítima, incluída como um serviço da nuvem computacional do *Maritime Services Cloud* (Marques, 2013) (NATO, 2012).

[20] CSM. "criação de saber acerca do espaço marítimo de ação ou de envolvimento com o objetivo de prever, identificar e localizar situações de interesse e propiciar a tomada de decisões atempadas e mais informadas" (Marques, 2013, p14)

O Exército centraliza a gestão e administração da sua rede, o Sistema de Informação e Comunicações Operacional (SIC-Op), no Regimento de Transmissões (RTm) em Lisboa. O SIC-Op divide-se em Rede de Dados do Exército (RDE), que são as redes locais que servem as Unidades, Estabelecimentos e Órgãos do Exército, e a Rede de Transmissão do Exército (RTE), que é uma rede de transporte que interliga as redes locais através de anéis de fibra ótica, ligações por feixes hertzianos e satélite. Dispõe de máquinas que controlam os acessos (*Network Access Control*), de antivírus de rede com atualizações automáticas, de *firewalls* (IXBOX) que permitem a coexistência da Internet com o SIC-Op. Para além da RDE classificada em "RESERVADO", existe uma "rede segura" que consiste em núcleos protegidos por equipamentos de cifra *Internet Protocol* da NATO nas principais salas de operações dos Comandos do Exército. Ao nível das redes táticas, o Sistema de Informação e Comunicações Tático (SIC-T) dispõe de equipamentos semelhantes, permitindo a projeção de módulos de comunicações em viaturas para o terreno, interligando-se ao SIC-Op ou eventualmente outro país aliado, através de um Ponto de Interoperabilidade (*Interoperability Point* – IOP) que respeita os STANAGs definidos no programa *Tactical Communications Post-2000* (TACOMS). O SIC-T é frequentemente testado no maior exercício de interoperabilidade do mundo, o *Combined Endeavor*, com mais de 40 países participantes.

A Força Aérea utiliza o SICOM para interligar as bases e unidades, onde são aplicadas "políticas de gestão e segurança administradas centralmente pela Direção de Comunicações e Sistemas de Informação" (Melo, 2011, p.23).

A nomeação de um dos ramos como Entidade Primariamente Responsável (EPR) para o desenvolvimento de uma capacidade de ciberdefesa teria todas as vantagens de um projeto em comum devidamente coordenado. O Exército parece ser o ramo que atualmente está com mais algum trabalho realizado neste campo, podendo constituir-se como EPR (Marques, 2013).

O segundo nível, "Grau de Contribuição dois" na figura três, justifica o esforço das FFAA na cibersegurança, quando o patamar de saturação das restantes entidades responsáveis pela cibersegurança ainda não foi atingido, mas que aceitem ser reforçadas ou receber a colaboração das FFAA. Assim, as operadoras das redes energéticas, de transporte, de telecomunicações, de distribuição de água, o sistema bancário, órgãos de soberania e de comunicação social que constituem a grande maioria das infraestruturas críticas nacionais, poderão receber o apoio das FFAA. A prioridade e alcance desta colaboração têm que ser claramente definidos, adequando-se a legislação em vigor, caso

necessário.

O terceiro nível, "Grau de Contribuição três" no topo da figura três, vê a cibersegurança enquadrada na Guerra da Informação[21], e mais concretamente nos níveis mais altos, os de Ciberguerra e de Guerra em Rede (Batista et al., 2003, p.39). Como vimos, os ciberataques podem ser disruptivos, de tal forma que as capacidades dos responsáveis naturais são excedidas. Ora as FFAA, "na defesa militar da República", são preparadas, equipadas e treinadas para conduzir operações ofensivas e defensivas, e deverão aceitar o desafio no domínio cibernético, contribuindo para colmatar a saturação de outros atores. A resposta ofensiva poderá materializar-se de várias formas, eventualmente com recurso a meios cinéticos, pelo que é uma exclusividade das FFAA. O Exército, por exemplo, já possui módulos táticos CIRC sedeados no RTm. O CNCDef no EMGFA parece ser a estrutura que será mais capaz de coordenar as atividades da futura capacidade de ciberdefesa nacional, podendo valer-se dos nossos aliados e das Organizações Internacionais, se necessário.

[21] "o conjunto de ações que visam preservar a integridade dos nossos sistemas de informação, evitando a sua exploração, corrupção ou destruição, por parte de adversários e, simultaneamente, executar ações que permitam explorar, corromper ou destruir os sistemas de informação dos adversários, obtendo-se assim vantagem de informação, no âmbito político, económico ou militar" (Batista et al., 2003, p.39)

Conclusões

Este trabalho iniciou com a definição de ciberespaço, um espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações e que é visto atualmente por muitos como um novo domínio da guerra. Este jovem ciberespaço, criação do Homem, que se quer livre e estável, precisa de ser operacionalizado, à imagem dos restantes domínios. Abundam as oportunidades, são facilitadas as interações, sem fronteiras, onde a imaginação é o limite. Com meio século de existência, conheceu um crescimento impressionante no qual florescem economias e sociedades. A nível militar, a dependência das FFAA mais modernas do frágil ciberespaço é notória, sendo este o palco de outras oportunidades, para atores menos escrupulosos. As ciberameaças são bem reais, variando segundo as suas caraterísticas, impactos, origens e atores, procurando atingir a disponibilidade, integridade e confidencialidade de um sistema. Quando são bem sucedidas, os efeitos podem ser catastróficos, como têm demonstrado alguns acontecimentos recentes, podendo levar um estado ao colapso. Assim, existem ciberataques cada vez mais complexos, capazes de ter um efeito disruptivo nos estados de tal ordem que todos os recursos disponíveis devem ser canalizados para repor a ordem interna e a normalidade. Porém, uma atitude preventiva e resiliente poderá suavizar este impacto.

São atualmente muitos os países que desenvolveram estratégias de cibersegurança, embora recentes, com estruturas adequadas à monitorização e proteção dos sistemas. Não existe uma definição concertada de cibersegurança, tendo a RU uma visão diferente do ocidente. Porém, pode-se propor agora a seguinte definição de cibersegurança: conjunto de medidas ativas e passivas que procuram proteger ou defender o ciberespaço. A ciberdefesa é assim um subconjunto da cibersegurança, que é mais abrangente.

Constatamos que a cibersegurança é uma prioridade para os cinco países estudados (EUA, NL, RU, RPC, UK), e para alguns encontra-se mesmo no topo das preocupações (EUA, UK, NL). Existem pontos em comum nas diversas estratégias analisadas: estas são relativamente recentes, aparecendo de forma mais consistente a partir de 2009. Todas visam a proteção no ciberespaço, a resiliência e há quem até sugira uma abordagem mais ofensiva (NL) na resposta aos ciberataques. Outro ponto de concordância é a necessária cooperação transversal dentro do setor público, interdepartamental e com o setor privado. Finalmente, é consensual a necessidade de inovar, criar conhecimento e educar as pessoas, o que pressupõe uma estreita ligação com as universidades. De forma genérica, uma boa estratégia deve definir claramente a estrutura de cibersegurança

implementada, com as responsabilidades delimitadas nos vários setores, e alargadas ao privado. Os países devem indicar com precisão o que desejam proteger, como se vão proteger e que capacidades são necessárias desenvolver. A cooperação internacional é igualmente vista como fundamental. É reconhecida a vontade dos estados mais avançados tecnologicamente, muito dependentes do ciberespaço, de alcançar uma maior prosperidade económica e social e para o efeito, precisam apartar as ciberameaças. Verificamos que as ciberameaças identificadas pelos países também têm similitudes: estados e atores não estatais, terroristas, criminosos, *hacktivistas* e atores internos. É de realçar que os EUA identificaram como ameaça as "atividades ainda não detetadas", reconhecendo que talvez seja uma das maiores, pois só *à posteriori* é que eventualmente se conhece a amplitude dos danos causados. Todavia, em relação ao contributo das FFAA na cibersegurança, foram notadas algumas discrepâncias, que resultam de dois motivos: a falta de transparência (RPC, RU, UK) e/ou a não disponibilização de dados em fontes abertas, por serem classificados. Os EUA e a NL são bastante claros, mas o UK e a RU afirmam que adotam uma postura unicamente defensiva. Porém, dos piores ataques da história foram associados por diversas vezes à RU e à RPC, e não parece expetável que o UK não disponha de uma capacidade ofensiva no ciberespaço.

O desenvolvimento de uma estratégia de cibersegurança enfrenta alguns dilemas que devemos tomar em linha de conta. Primeiro, tem que existir um equilíbrio que é difícil, entre dar a maior liberdade possível no ciberespaço para estimular a economia e respeitar a liberdade dos cidadãos e por outro lado, garantir uma proteção apropriada. A RPC resolveu este dilema com a adoção do *Muro da China,* e um controlo apertado sobre todas as atividades no ciberespaço. Em segundo lugar, a modernização das infraestruturas críticas, numa dependência crescente nas tecnologias e sistemas de informação, é desafiante para quem pretenda a sua proteção. Neste âmbito, são normalmente mantidos sistemas mais antigos em reserva. Em terceiro lugar, é fundamental uma maior parceria entre o setor privado que estuda, desenvolve e implementa as tecnologias, com o setor público onde residem os serviços essenciais e as capacidades críticas. Outro dilema relaciona-se com a necessidade de partilha da informação e a sua proteção. A título de exemplo, os sistemas de C2 permitem uma planificação do campo de batalha mas estão sujeitos à erosão tecnológica do adversário (Klimburg, 2012, pp.34-41).

Além da participação ativa entre entidades a nível interno, a cooperação internacional é maioritariamente sublinhada. Analisamos a postura de três Organizações Internacionais das quais Portugal é membro (NATO, UE e ONU) em relação à

cibersegurança, concluindo que existe uma preocupação crescente e que a cooperação com vista a enfrentar as ciberameaças é incentivada.

A NATO reconheceu na cimeira de Lisboa que a ciberdefesa era importante e o Processo de Planeamento da NATO seria o instrumento impulsionador de capacidades de ciberdefesa dentro das nações. Contudo, esta na moda o conceito de *Comprehensive Approach*, onde se pretende englobar na equação os outros instrumentos de poder com parte da solução, o que se enquadra perfeitamente no espírito colaborativo, sendo necessário manter este pensamento na análise, planeamento e execução. Por outro lado, a NATO estimula a CFI para manter a prontidão, eficiência e interoperabilidade e uma *Smart Defence* no seio dos aliados, abrindo oportunidades para desenvolver, com custos menores, interoperáveis e eficientes, capacidades de ciberdefesa por exemplo. São óbvias as vantagens, mas não isentas de responsabilidades, pois fazendo uma analogia culinária, "não se retira uma fatia do bolo comum sem contribuir com ingredientes também". As capacidades técnicas têm todo o interesse de ser desenvolvidas em conjunto, de forma a dimimuir o custo, facilitar a interoperabilidade e eficiência (Jordan et al., 2012, pp.164-65).

A UE tem uma abordagem menos militar dos assuntos, com uma estratégia de cibersegurança recente que não é inovadora. A crise económica que atravessamos obrigou os estados-membros a cooperar, fomentando o *Pooling and Sharing*. Uma maior cibersegurança comum, traduz-se numa melhor cibersegurança interna, e as FFAA são um dos elementos incontornáveis dos estados participativos neste esforço e facilitador da cooperação que se habituou a aprimorar ao longo do tempo nas diversas missões militares internacionais.

Em relação à ONU, existe igualmente a vontade de uma maior cooperação entre as nações, embora fossem salientadas diferenças conceituais entre os que procuram o desenvolvimento de capacidades de cibersegurança e os que preferem progressos legislativos. A ITU recomenda alguns elementos que podem fazer parte de uma estratégia de cibersegurança, sendo por isso uma boa referencia a tomar em conta por Portugal.

Portugal ainda não tem uma estratégia para o ciberespaço embora existam vários trabalhos académicos que abordam o assunto, com óbvias similitudes com as estratégias estudadas na investigação. No recente CEDN, o desenvolvimento de "capacidades militares necessárias à mitigação das consequências de ataques (...) cibernéticos" é uma prioridade, por isso, está previsto o levantamento de uma capacidade de ciberdefesa nacional. Se a cibersegurança é essencialmente uma responsabilidade das FFSS em relação ao cibercrime e ao hacktivismo, no que diz respeito à ciberespionagem e ao ciberterrorismo

a responsabilidade é dos Serviços de Informação. As FFAA podem contribuir quando a capacidade de resposta destas entidades estiver a ser excedida. O futuro CNCSeg, na dependência direta do PM, será o pulmão agregador de todas as entidades de cibersegurança nacionais.

As FFAA têm a exclusividade da ciberdefesa, conduzindo ciberoperações numa vertente defensiva e ofensiva, quando se estiver no limiar do colapso da nação. No entanto, antes de se atingir este patamar (Grau três), foram identificados outros dois preliminares, com graus de contribuição diferentes das FFAA (figura 3): no primeiro (Grau um), as FFAA são um ator participativo no esforço global de cibersegurança, responsável por manter seguro o ciberespaço que é da sua jurisdição e gestão; no segundo (Grau dois), as FFAA como colaboradoras, em apoio das FFSS e Serviços de Informação.

Já é possível recomendar algumas medidas para cada um dos três patamares de disrupção visualizados.

Em relação ao "Grau um" de contribuição das FFAA, no dia a dia, onde as ciberameaças não têm um impacto significativo:

- ✓ Cultura de cibersegurança;
- ✓ Auto proteção;
- ✓ Simulação e Exercícios.

A responsabilidade de segurança no ciberespaço inicia-se com a intervenção individual, onde cada um deve tomar as medidas necessárias ao seu nível, e para este efeito, deverá estar sensibilizado para estas questões. Deve nascer e florescer uma cultura da cibersegurança no seio das FFAA. Para o efeito, podem ser conduzidas ações de formação e palestras sobre a temática, difundidas mensagens de alerta sobre as ciberameaças e encorajadas as boas práticas, através do correio eletrónico por exemplo.

Contribuir para a cibersegurança do todo, garantindo a segurança das suas próprias redes de telecomunicações e sistemas de informação: a auto proteção. O EMGFA deve elaborar uma Política de Segurança suportada por normas internacionais e STANAGs. Ao nível dos ramos, deverão estar implementadas boas práticas transversais sob orientação do EMGFA, com procedimentos detalhados. Sugere-se ainda, que seja eventualmente pedido à Autoridade Nacional de Segurança a certificação das redes, garantindo o respeito das normas estabelecidas a nível nacional. O CNCDef deverá monitorizar a atividade nas redes e reportar ao CNCSeg, que poderá ter pelo menos um elemento militar.

Já referia Sun Tzu, "na paz, prepara-te para a guerra". Ao nível do CNCSeg, devem ser elaborados cenários que justifiquem o emprego das FFAA, desenvolvidos planos detalhados e conduzidos exercícios de treino, com eventual recurso a ferramentas de simulação para teste dos planos.

No grau dois de contribuição das FFAA, quando as ciberameaças são já significativas

- ✓ Colaboração interna
- ✓ Integração no Sistema de Proteção da Infraestrutura de Informação Nacional
- ✓ Legislação clarificadora

As FFAA podem colaborar com os responsáveis pelas infraestruturas críticas nacionais, reforçando-os com peritos, disponibilizando técnicos qualificados *"on-call"*. O objetivo é fortalecer as capacidades convencionais para em conjunto, exponenciar os efeitos sobre os ciberataques.

A colaboração justifica-se existir com o setor privado uma vez que as infraestruturas de transporte de comunicações estão nas mãos de privados, nomeadamente as operadoras de telecomunicações como a Portugal Telecom, por exemplo. Todavia, os dados do setor público, FFAA incluídas, viajam diariamente por estas auto estradas da informação, com larguras de banda sempre maiores. Assim, é fundamental a confiança mútua e a cooperação entre estes dois setores mas carecem da criação de um modelo enquadrador com responsabilidades bem definidas. Recomenda-se que as FFAA sejam parte integrante do futuro SPIIN.

Em termos legislativos, deve ser clarificada a cooperação "com as forças e serviços de segurança tendo em vista o cumprimento conjugado das respetivas missões no combate a agressões ou ameaças transnacionais" (AR, 2009) com a emanação de uma Resolução do Conselho de Ministros.

No grau três de contribuição das FFAA, quando as ciberameaças põem em causa a nação.

- ✓ CNCDef como órgão coordenador principal da cibersegurança
- ✓ Definição de Regras de Empenhamento
- ✓ Cooperação internacional

Em *Wars of disruption and resilience*, a doutora Demchak aconselha que na defesa, se deve dificultar a tarefa dos piratas informáticos tornando mais oneroso e ariscado a realização de ataques e menos acessíveis as ferramentas de ataques. Para isso devem as instituições públicas (defesa, FFSS, serviços de informação) partilhar conhecimentos entre elas e com as operadoras. Demchak defende que as FFAA, num mundo cibernético, têm um papel crítico na resiliência como salvadoras das sociedades, tanto como o fazem em operações cinéticas (Demchak, 2011). As FFAA são reconhecidas pela sua capacidade de planeamento, e com a concretização do levantamento futuro de uma capacidade de ciberdefesa, recomenda-se uma subordinação do CNCSeg ao CNCDef, numa situação de grau três ou, em alternativa, o reforço do CNCSeg com pessoal militar.

Levantar uma capacidade significa seguir o preconizado pela sigla DOTMLPFI (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade) para efetivamente ser uma realidade. A futura capacidade de ciberdefesa, além deste aspeto e para ser aplicada numa situação de grau três, carece de Regras de Empenhamento precisas.

À imagem das ameaças, que podem ser transnacionais, a cooperação deve ser entre estados a fim de dar uma resposta adequada. "A União Europeia e a OTAN são vitais para a segurança e defesa nacionais" (RCM, 2013a, p.6). Portugal, na ligação e complementaridade que é obrigado a manter entre as organizações, deve ser inteligente para poder aproveitar, em relação ao ciberespaço, a cooperação que hoje é procurada por todos. Não pode perder a oportunidade para, de acordo com as orientações políticas, seguir uma estratégia vantajosa, participando nos projetos mais benéficos, adequados à dimensão do nosso país, como o "projeto multinacional de desenvolvimento de capacidades de ciberdefesa" e, desejavelmente, contribuir para não deixar nenhuma capacidade crítica nas mãos de um único parceiro. O peso específico de Portugal diminui com o alargamento da NATO a outros países e o afastamento declarado dos EUA para o Pacífico. Podemos contribuir para missões em áreas que fazem a diferença, apostando no desenvolvimento de capacidades em ambiente internacional que sirvam para o bem da aliança. Existem hoje oportunidades a explorar e que servem tanto a nível interno, para o cumprimento das missões de soberania, como para o preenchimento de nichos de excelência nas Organizações Internacionais, contribuindo de forma clara para o todo.

Concretização das recomendações

As recomendações apresentadas podem ser concretizadas no tempo de forma diferenciada e necessitam de recursos variáveis, para atingir os efeitos pretendidos. É seguramente mais rápido e menos oneroso implementar as medidas independentes da aquisição de novos equipamentos e dependentes da alteração de processos: integração das FFAA na SPIIN, alterações legislativas, regras de empenhamento enquadram-se neste grupo de curto prazo. A seguir, a médio prazo, consegue-se alcançar uma cultura de cibersegurança, uma auto proteção e a criação de um CNCDef coordenador pois estas medidas carecem de algum tempo para atingir os efeitos: não se muda mentalidades rapidamente, nem se acredita uma rede ou se criam capacidades tão facilmente. No longo prazo, e com custos igualmente maiores, é que se podem conduzir exercícios e simulações, atingir uma plena colaboração interna e cooperação internacional pois depende da total operacionalidade da capacidade de ciberdefesa das FFAA como contribuinte para a cibersegurança nacional.

Bibliografia

ACT, 2013. *Assured Access to the Global Commons*. [Online] Available at: http://www.act.nato.int/mainpages/globalcommons [Accessed fevereiro 2013].

ANACOM, 2011. *Quem somos*. [Online] Available at: http://www.anacom.pt [Accessed abril 2013].

ANETIE, 2012. *Missão e objetivos*. [Online] Available at: http://www.anetie.pt/website.aspx?p=191 [Accessed março 2013].

APRITEL, 2013. *Missão e objetivos*. [Online] Available at: http://www.apritel.org/gca/index.php?id=16 [Accessed março 2013].

AR, 2009. Lei Orgânica de Bases da Organização das Forças Armadas. *Diário da República*, 7 Julho.

Arreguín-Toft, I., 2001. How the Weak Win Wars. *International Security*, 26(1), pp.93-128.

Assembleia da República, 2004. Lei de organização e funcionamento da Comissão Nacional de Proteção de Dados. *Diário da República*, 18 agosto.

Assembleia da República, 2008. Lei de Organização da Investigação Criminal. *Diário da República*, 17 agosto. Lei nº48/2008 de 27 de agosto.

Assembleia da República, 2008. Lei nº53/2008 - Lei de Segurança Interna. *Diário da República*, 29 agosto.

Batista, Ribeiro & Amaral, 2003. Ciberterrorismo: a nova forma de crime do séc. XXI , como combatê-la? *Proelium Academia Militar*.

Benitez, J., 2013. *Russian army to create its own cyber command*. [Online] Available at: http://www.acus.org/natosource/russian-army-create-its-own-cyber-command [Accessed março 2013].

Cabinet Office UK, 2011. *The UK Cyber Security Strategy*.

Cabinet Office, 2012. *National Security Council*. [Online] Available at: http://www.cabinetoffice.gov.uk [Accessed janeiro 2013].

Carr, J., 2011. *7 reasons why China isn't the world's biggest threat*. [Online] Available at: http://jeffreycarr.blogspot.pt/2011/06/7-reasons-why-china-isnt-worlds-biggest.html?q=Russian+cyber+operations+are+rarely+discovered [Accessed março 2013].

CERT.PT, 2013. *Missão*. [Online] Available at: http://www.cert.pt [Accessed abril 2013].

CERT-EU, 2013. *RFC 2350*. RFC. Computer Emergency Response Team.

Chen, Z., 2010. La stratégie militaire "asymétrique" de la Chine. *Études internationales*, 41(4), pp.547-69.

Clarke, R., 2010. *Cyberwar - The next threat to National Security and what to do about it*. New York: HarperCollins.

CNAS, 2013. *Contested commons*. [Online] Available at: http://www.cnas.org/contestedcommons [Accessed janeiro 2013].

CNCERT, 2009. *About us*. [Online] Available at: http://www.cert.org.cn/ [Accessed fevereiro 2013].

Comissão Europeia, 2013. *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace*. comunicação. Bruxelas: União Europeia.

Conselho de Ministros 6/2003, 2003. Conceito estratégico de defesa nacional. *Diário da República*, 20 janeiro.

Crowell, R., 2012. *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare*. paper. Naval War College.

CSIRT.FEUP, 2013. [Online] Available at: http://csirt.fe.up.pt [Accessed março 2013].

Decreto Russo, 2009. *Russia's National Security Strategy to 2020*. [Online] rustrans Available at: http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020 [Accessed março 2013]. traduzido para inglés e disponível em http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020.

Demchak, C., 2011. *Wars of disruption and resilience – cybered conflict, power, and national security*. Georgia, EUA: University of Georgia Press.

Department of Defense, 2011. *Department of Defense Strategy for Operating in Cyberspace*. DoD.

DHS,DoD, 2010. *MEMORANDUM OF AGREEMENT BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY*. memorando de entendimento. DHS;DoD.

ECNS, 2012. *PLA Online Blue army gets ready for cyber warfare*. [Online] Available at: http://www.ecns.cn/2012/01-16/6254.shtml [Accessed fevereiro 2013].

ENISA, 2012. *Cyber Europe 2012 key findings and recommendations*. recomendações. ENISA.

ENISA, 2013. *Mission*. [Online] Available at: http://www.enisa.europa.eu/about-enisa/activities/mission [Accessed março 2013].

Europa, 2010. *Política de segurança e de defesa comum*. [Online] Available at: http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty [Accessed novembro 2012].

European Defence Agency, 2012. *About us*. [Online] Available at: http://www.eda.europa.eu [Accessed dezembro 2012].

Exército Português, 2012. *PDE 3-00 Operações*.

Faleg & Giovannini, 2012. 61 *The EU between Pooling & Sharing and Smart Defence*. paper.

FCCN, 2013. *Missão e visão*. [Online] Available at: http://www.fccn.pt/pt/a-fccn/o-que-e-a-fccn/missao-e-visao/ [Accessed março 2013].

GCHQ, 2013. *GCHQ homepage*. [Online] Available at: http://www.gchq.gov.uk [Accessed janeiro 2013].

Giles, K., 2012. Russia and Cyber Security. *Nação e Defesa*, 133(5), pp.69-88.

GNS, 2012. *Gabinete Nacional de Segurança*. [Online] Available at: http://www.gns.gov.pt/gns/pt/missao/ [Accessed março 2013].

GNS, n.d. *Proposta de Estratégia Nacional de Cibersegurança*. proposta. Gabinete Nacional de Segurança.

Government, 2010. *The National Security Strategy*. Londres: HM Government.

Harris, S., 2010. *All in one CISSP exam guide*. 5th ed. McGraw-Hill.

Honorato, M., 2012. Cibersegurança em Portugal: aonde nos encontramos? Lisboa, 2012.

House of Commons Defence Committee, 2013. *Defence and Cyber-Security*. 6th Report. Authority of the House of Commons.

Huang, A.C.-c., 2001. Transformation and refinement of Chinese Military Doctrine: Refelection and critique on the LA's view. In R. Corporation, ed. *Seeking truth from facts*. pp.131-40.

Internetworldstats, 2013. *Internet World Stats*. [Online] Available at: http://www.internetworldstats.com [Accessed janeiro 2013].

ISO, 2012. *ISO/IEC 27032 Information technology - security techniques*. Standard. International Organization for Standardization.

ITU, 2013. *What does ITU do?* [Online] Available at: http://www.itu.int/en/about/Pages/whatwedo.aspx [Accessed março 2013].

Joint Chiefs of Staff, 2011. *JP 3-0 Joint Operations*.

Joint Chiefs of Staff, 2012. *JP 3-13 Information Operations*.

Jordan, Hallingstad & Szydelko, 2012. Towards Multi-national Capability Development in Cyber Defence. *Nação e Defesa*, 133(5), pp.154-66.

Klimburg, A., 2012. *Nato Cyber Security Framework Manual*. manual. Tallin: NATO CCDCOE.

Kohl, D., 2013. NATO Reform update. Bruxelas, 2013. conferência no decorrer da visita do CEMC ao NATO HQ.

Lam, W., 2010. Beijing bones up its cyber-warfare capacity. *China Brief - a journal of analysis and information*, 10(3).

Liang & Xiangsui, 1999. *Unrestricted Warfare*. Pequim: PLA literature and Arts Publishing House.

Libicki, M., 2012. Cyberspace is not a warfighting domain. *Journal of law and policy for the information society*, 8(2), pp.325-40.

Lindsay, J., 2012. *China and Cybersecurity: Political, Economic, and Strategic Dimensions*. relatório de um workshop. San Diego: University of California.

Luís, A., 2013. Conferencia do Secretário Geral do Sistema de Segurança Interna. Pedrouços, 2013. 23Jan13 no IESM.

Marques, G., 2013. Cibersegurança e conhecimento situacional marítimo. *Revista da Armada*, 472.

Marques, G., 2013. *Entrevista ao Sr. CALM Gameiro Marques*. Entrevista. Lisboa. 04 abril 2013.

Melo, P., 2011. *A CIBERGUERRA. ESTRUTURA NACIONAL PARA ENFRENTAR AS VULNERABILIDADES – UMA CAPACIDADE MILITAR AUTÓNOMA OU PARTILHADA.*. TII. IESM.

metac0m, 2003. *What is hacktivism? 2.0*.

MGI, 2011. *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*. estudo. McKinsey Global Institute.

Ministerie van Defensie, 2012. *The Defence Cyber Strategy*. estratégia. Haia: Ministerie van Defensie.

Ministry of Security and Justice, 2011. *The National Cyber Security Strategy*. estratégia. Haia.

NATO, 2010. *Strategic concept for the defence and security of the members of NATO*. conceito estratégico. Lisboa: NATO.

NATO, 2011. *Defending the networks - The NATO policy on Cyber Defence*. política. Bruxelas: NATO.

NATO, 2012. *AAP-06 NATO Glossary of terms and definitions*. 20122nd ed.

NATO, 2012. *Smart Defence*. [Online] Available at: http://www.nato.int/docu/review/Topics/EN/Smart-Defence.htm [Accessed janeiro 2013].

NATO, 2012. *Summit Declaration on Defence Capabilities: Toward NATO Forces 2020*. [Online] Available at: http://www.nato.int/cps/en/natolive/official_texts_87594.htm?mode=pressrelease [Accessed abril 2013].

NATO, 2013. *NATO and cyber defence*. [Online] Available at: http://www.nato.int/cps/en/natolive/topics_78170.htm [Accessed março 2013].

NATO, 2013. *NATO Nations launch multinational cyber defence project*. [Online] Available at: http://www.ncia.nato.int/news/Pages/130315-MNCD2.aspx [Accessed março 2013].

NCIA COS, 2013. NCIA Agency. Bruxelas, 2013. Visita de estudo do CEMC à Bélgica.

NCSC, 2012. *Cyber Security Assessment Netherlands*. avaliação. Haya: National Cyber Security Centre.

NCSC, 2012. *National Cyber Security Centre Organisation*. [Online] Available at: https://www.ncsc.nl/english/organisation [Accessed fevereiro 2013].

NSA, 2011. *Mission*. [Online] Available at: http://www.nsa.gov/about/mission/index.shtml [Accessed janeiro 2013]. National Security Agency.

Nunes, P.V., 2012. A definição de uma Estratégia Nacional de Cibersegurança. *Nação e Defesa*, 133(5ª), pp.113-27.

ODKB, n.d. *Организация Договора о коллективной безопасности*. [Online] Available at: http://www.odkb.gov.ru/start/index_aengl.htm [Accessed março 2013].

OECD, 2012. *Cybersecurity Policy Making at a Turning Point*. OECD Publishing.

ONU, 2011. *Potential Threats Can 'Provoke Outbreak of Large-scale Information Wars'*. Meeting. Nova Iorque: ONU.

Pastor, Q., 2013. Portugal na NATO e na UE. Bruxelas, 2013. Visita de estudo à Bélgica do CEMC.

Pinto, L.P., 2013. Conferência do Diretor Geral do Seerviço de Informações de Segurança. Pedrouços, 2013. IESM 24Jan13.

PJ, 2013. *Unidade nacional de combate à corrupção*. [Online] Available at: http://www.policiajudiciaria.pt [Accessed abril 2013].

Posen, B., 2003. Command of the Commons. *International Security*, 28(1).

Raymond, E., 2000. *The new hacker's dictionary*. 4th ed. The MIT press.

RCM, 2013a. *Conceito Estratégico de Defesa Nacional*. Resolução Conselho de Ministros. Lisboa.

RCM, 2013b. Resolução do Conselho de Ministros nº26/2013. *Diário da República*, 1(77).

Robinson, Gribbon, Horvath & Robertson, 2013. *Cyber-security threat characterisation*. paper. RAND Europe.

Ruhle, M., 2013. The emerging security landscapes: challenges for NATO. Bruxelas, 2013. VIsita de estudo à Bélgica do CEMC - NATO HQ.

Russian Armed Forces, 2011. *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. estratégia. Вооружённые Си́лы Росси́йской Федера́ции.

Shaw, D., 2010. *Cyberspace: What senior military leaders need to know*. US Army War College.

Smith, D., 2012. *Russian Cyber Operations*. Potomac Institute Cyber Center.

UK Parliament, 2012. *Defence and Cybersecurity*. [Online] Available at: http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/writev/1881/dcs01.htm [Accessed janeiro 2013].

UMIC, 2006. *sobre a UMIC*. [Online] Available at: www.umic.pt [Accessed abril 2013].

União Europeia, 2012. *Agências da UE*. [Online] Available at: http://europa.eu/agencies/regulatory_agencies_bodies/security_agencies/eda/index_pt.htm [Accessed dezembro 2012].

UNODA, 2010. *Developments in the field of information and telecommunications in the context of international security*. [Online] Available at: http://www.un.org/disarmament/topics/informationsecurity/ [Accessed março 2013]. A/65/201 Groups of Governmental Experts.

US Air Force, 2013. *Our Mission*. [Online] Available at: http://www.airforce.com/learn-about/our-mission/ [Accessed janeiro 2013].

USSTRATCOM, 2010. *Mission*. [Online] Available at: http://www.stratcom.mil [Accessed janeiro 2013].

Vacca, A., 2011. Military Culture and Cyber Security. *Survival - Global Politics and Strategy*, 02 dezembro. pp.159-76.

Wamala, F., 2011. *The ITU National Cybersecurity strategy guide*. guia. International Telecommunication Union.

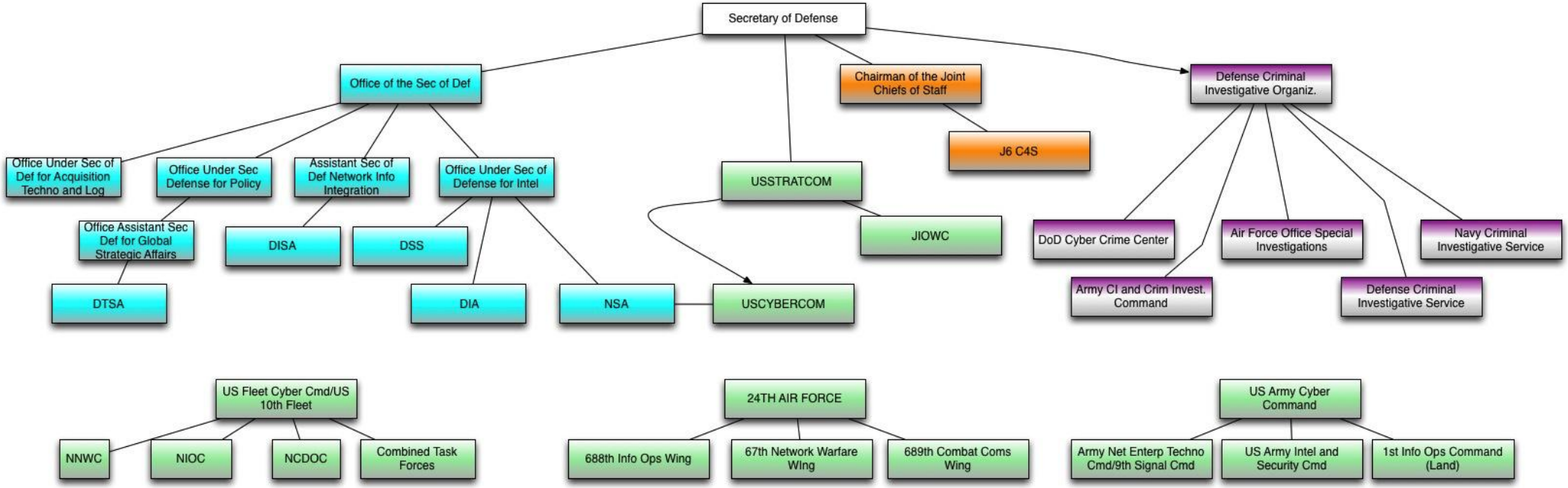
Anexo A – Modelo de análise

CONCEITO	DIMENSÕES	INDICADORES
CIBERSEGURANÇA	Estratégia	Existe? Revisões? Quem elaborou? As ameaças levantadas Pontos principais
	Entidades responsáveis	Setor Publico Setor Privado
	Contributos FFAA	Estrutura Efetivos Maturidade Colaboração ou cooperação com outros setores

Anexo B – Documentos relacionados com cibersegurança por país

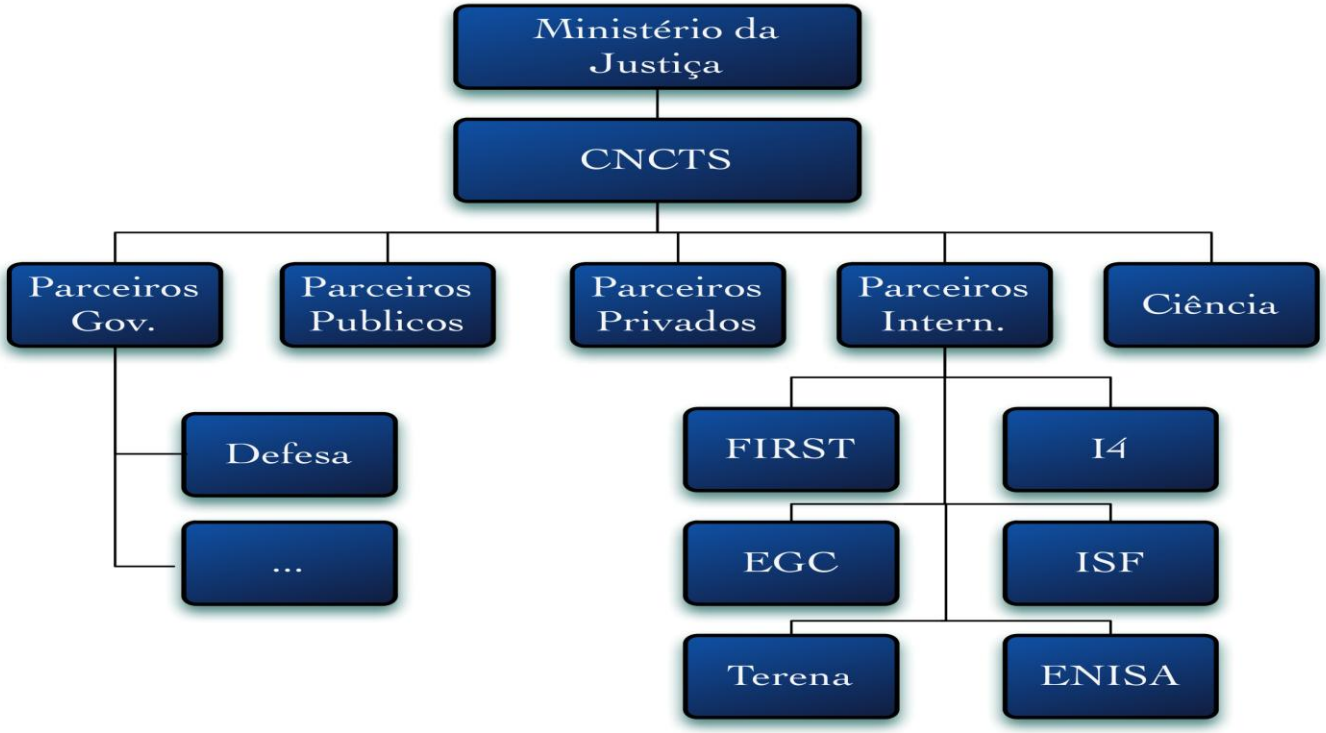
China	• *Unrestricted Warfare,* 1999 • Documento 27
Estados Unidos	• Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. White House, 2009. • International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. White House, 2011. • Cybersecurity Legislative Proposal. White House, 2011. • Comprehensive National Cybersecurity Initiative. White House, 2010. • Department of Defense Strategy for Operating in Cyberspace. Department of Defense, 2011. • Cybersecurity, Innovation and the Internet Economy. Department of Commerce, 2011. • National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security and Privacy. White House, 2011. • Trustworthy Cyberspace: Strategic Plan for the Federal cybersecurity Research and Development Program. Executive Office of the President, National Science and Technology Council, 2011.
Holanda	The National Cyber Security Strategy. Dutch Ministry of Security and Justice, 2011
Reino Unido	• The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. UK Cabinet Office, 2011. • Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space. UK Cabinet Office, 2009. • Strategic Defence and Security Review (SDSR). UK Prime Minister, 2010. • A Strong Britain in an Age of Uncertainty: The National Security Strategy. UK Prime Minister, 2010. • Cyber Crime Strategy. Home Office, 2010.
Russia	• A doutrina de segurança da informação da RU, 2009 • Visões conceptuais em relação às atividades das Forças Armadas da Federação Russa no espaço da informação, 2011

Anexo C – Estrutura organizacional de cibersegurança dos EUA



Adaptado de http://prezi.com/xvyiaa-gkb8h/copy-of-us-dod-cyber-organizational-structure/

Anexo D – Estrutura organizacional de cibersegurança de NL



CNCTS: Coordenador Nacional para o Contra Terrorismo e a Segurança
NCSC: Centro Nacional de Cibersegurança
FIRST: Forum of Incident Response and Security Teams
EGC: European Government CERTs
Terena: Trans European Research and Education Networks Association
I4: International Information Integrity Institute
ISF: Information Security Forum
ENISA: European Network and Information Security Agency

Anexo E – Estrutura organizacional de cibersegurança do UK