INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE ESTADO-MAIOR CONJUNTO

2011/2012

TII

SEGURANÇA E DEFESA NACIONAL:

O DESENVOLVIMENTO DE CAPACIDADES DE CIBERDEFESA

VERSÃO PROVISÓRIA

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

NUNO ANDRÉ BARROS MONTEIRO DA SILVA

CAPITÃO PILOTO-AVIADOR

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

SEGURANÇA E DEFESA NACIONAL: O DESENVOLVIMENTO DE CAPACIDADES DE CIBERDEFESA

Cap PILAV Nuno Monteiro da Silva

Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto 2011/2012

VERSÃO PROVISÓRIA

Lisboa, 2012

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

SEGURANÇA E DEFESA NACIONAL: O DESENVOLVIMENTO DE CAPACIDADES DE CIBERDEFESA

Cap PILAV Nuno Monteiro da Silva

Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto 2011/2012

Orientador: TCor ENGEL Armando Barros

Lisboa, 2012

Agradecimentos

A realização deste trabalho só foi possível com a ajuda de várias pessoas, às quais não posso, nem quero, deixar de agradecer:

À Força Aérea Portuguesa que me tornou no que sou hoje e me deu as ferramentas para atingir os meus objetivos. A todos os que direta ou indiretamente contribuíram para o meu conhecimento e para a minha formação académica, militar e operacional.

Ao meu orientador, TCor ENGEL Armando Barros, pela sua preciosa ajuda, apoio, disponibilidade, paciência e amizade.

Em especial:

À minha mulher, Catarina e às minhas filhas, Filipa e Sofia, que são os pilares da minha existência e a minha fonte de motivação última, pela sua compreensão e apoio incondicional.

Ao meu irmão, pela sua assertividade e vincado profissionalismo, que se juntam às suas qualidades humanas e sentido de família, sendo um exemplo para mim.

À minha mãe, pelo seu apoio incondicional ao longo da minha vida e pelo seu exemplo de força e determinação nos momentos mais difíceis e desafiantes das nossas vidas.

Ao meu pai, pela sua inteligência, inspiradora capacidade de trabalho e sentido de dever, que nunca deixará de existir na minha memória e nas minhas ações como pessoa e oficial das Forças Armadas e a quem dedico este trabalho.

Indíce

Lista de figuras e tabelas

Resumo

A internet como criação humana que é encerra em si falhas e imperfeições, do ponto de vista da segurança, que podem ser aproveitadas para atividades ilícitas, espionagem, terrorismo ou mesmo para perpetrar ataques que tenham como alvo estruturas civis, governamentais ou militares. Surgem desta forma, diversos conceitos precedidos pela palavra "ciber" e que procuram explicar e compreender as muitas formas de interação lícita e ilícita, amiga e inimiga, pacífica ou belicista que este novo "mundo" virtual origina.

Como consequência, assistimos à instrumentalização do ciberespaço para fins estritamente militares, materializada, por exemplo, na criação de um *Cyber Command* pelos Estados Unidos da América, tendo-se tornado importante o balanço ótimo entre capacidades de defesa e potencialidades para ataque.

Internacionalmente, também a União Europeia, as Nações Unidas, a Organização do Tratado do Atlântico Norte e os inúmeros organismos internacionais a estas associados, têm dado ênfase a este novo domínio. É patente a sua transversalidade, que acompanha a galopante evolução tecnológica das últimas décadas, e que se estende agora a todos os setores - sejam eles civis, estatais ou militares - onde o processamento de informação excede a capacidade humana, constituindo-se a ligação em rede das principais infraestruturas críticas, como verdadeiros *high-value assets* que requerem proteção e defesa contra intrusões.

A articulação entre estes diferentes setores torna-se premente para o desenvolvimento de uma estratégia da informação holística e capaz. A nível nacional várias entidades desenvolvem já esforços no âmbito da cibersegurança, não existindo no entanto, uma estratégia nacional que permita o desenvolvimento das sinergias necessárias para uma eficaz e cabal proteção.

O presente trabalho procura analisar as diferentes estruturas de ciberdefesa existentes e consolidadas a nível internacional, de forma a concetualizar um modelo nacional para uma estrutura de ciberdefesa holística e transversal. Para tal, recorreu-se ao método de investigação em ciências sociais proposto por Quivy e Campenhoudt.

Assim, foram identificadas diversas vulnerabilidades a nível nacional no âmbito da ciberdefesa, procurando-se compreender de que forma as principais organizações internacionais com que Portugal se relaciona, desenvolvem os seus esforços neste domínio, permitindo elencar as capacidades a desenvolver no nosso país, mostrando, neste sentido, a necessidade de trabalhar em conjunto, com a sociedade civil e os parceiros internacionais.

Abstract

The Internet as a human creation encloses flaws and imperfections, from the point of view of security, that can be used for illicit activities, espionage, terrorism or even to perpetrate attacks targeting civilian, governmental or military structures.

Several concepts arose preceded by the word "cyber" seeking to explain and understand the many forms of licit and illicit, peaceful or harmful interactions that this new virtual "world" encloses.

We see the exploitation of cyberspace for strictly military purposes, materialized, for example, in the creation of a Cyber Command by the United States of America, where understanding of the optimal balance between defense capabilities and potential for attack is required.

Internationally, also the European Union, the United Nations, the North Atlantic Treaty Organization and numerous international organizations associated with these, have done so. Patent is the transversally of this new field, which accompanies the technological savvy of the last decades, extending to all sectors - be they civilian, military or state - where the information processing exceeds human capacity, transforming the main critical network infrastructures into true high-value assets that require protection and defense against intrusion.

Reconciling these different sectors is urgent to develop a holistic and capable information strategy. At the national level, various entities have developed cyber-security efforts, however, a national strategy that allows the creation of synergies necessary to ensure an effective and complete protection is in order.

This paper analyzes the different and consolidated cyber-defense structures that exist at an international level in order to create a national model for a holistic and transversal cyber-defense structure. In order to achieved this, the Quivy e Campenhoudt Social Sciences Investigation Method was used.

This investigation identifies several vulnerabilities at the national level in the cyber defense domain, and seeks to understand the path followed by the main international organizations with which Portugal relates to, in order to point out the capabilities to be developed in our country, showing, in this matter, the need for joint work in cooperation with the civilian society and the international partners.

Palavras-Chave

Centro Nacional de Cibersegurança, Ciberataque, Ciberdefesa, Ciberespaço, Estratégia Nacional de Segurança da Informação, Infraestrutura Crítica Nacional, Infraestrutura da Informação Crítica Nacional, Tecnologias da Informação e Comunicação.

Lista de abreviaturas, siglas e acrónimos

ACO	*Allied Command Operations*
ACT	*Allied Command Transformation*
ANACOM	Autoridade Nacional de Comunicações
ANS	Autoridade Nacional de Segurança
CCDCoE	*NATO Cooperative Cyber Defense Centre of Excellence*
CE	Comissão Europeia
CEGER	Centro de Gestão da Rede Informática do Governo
CEMFA	Chefe do Estado-Maior da Força Aérea
CERT	*Computer Emergency Response Team*
CNA	*Computer Network Attack*
CNC	Centro Nacional de Cibersegurança
CND	*Computer Network Defense*
CNO	*Computer Network Operations*
CPLP	Comunidade de Países de Língua Portuguesa
CRISI	Capacidade de Resposta a Incidentes de Segurança Informática
CRP	Constituição da República Portuguesa
CSI	Comunicações e Sistemas de Informação
CSIRT	*Computer Security Incident Response Team*
CYBERCOM	*Cyber Command*
DDoS	*Directed Denial of Service*

DoS	*Denial of Service*
DNS	*Domain Name Service*
ECEE	Entidade de Certificação Eletrónica do Estado
EUA	Estados Unidos da América
EUROJUST	Unidade Europeia de Cooperação Judiciária
EMFA	Estado-Maior da Força Aérea
EMGFA	Estado-Maior General das Forças Armadas
ENC	Estratégia Nacional de Ciberdefesa
ENSI	Estratégia Nacional de Segurança da Informação
EW	*Electronic Warfare*
FAP	Força Aérea Portuguesa
FCCN	Fundação para a Computação Científica Nacional
FFAA	Forças Armadas
FFCI	*Framework for Collaborative Interaction*
FND	Forças Nacionais Destacadas
GPTIC	Grupo de Projeto para as TIC
GRISI	Grupo de Resposta a Incidentes de Segurança Informática
I2CN	Infraestrutura da Informação Crítica Nacional
ICE	Infraestrutura Crítica Europeia
ICN	Infraestrutura Crítica Nacional
IDN	Instituto de Defesa Nacional
IDS	*Intrusion Detection System*

ISP	*Internet Service Provider*
IESM	Instituto de Estudos Superiores Militares
MAI	Ministério da Administração Interna
MDN	Ministério da Defesa Nacional
MEC	Ministério da Educação e Ciência
MILDEC	*Military Decepcion*
NCI	*National Critical Infrastructure*
NCIRC	*NATO Computer Incident Response Capability*
OPSEC	*Operations Security*
OSCE	Organização para a Segurança e Cooperação Europeia
OSI	*Open Systems Interconnection*
OTAN	Organização do Tratado do Atlântico Norte
PEPIC	Programa Europeu de Proteção das Infraestruturas Críticas
PPP	Parcerias Público-Privadas
PSP	Polícia de Segurança Pública
PSYOPS	Operações Psicológicas
PT	Portugal Telecom
RoE	*Rules of Engagemente*
RTIR	*Request Tracker for Incident Response*
SCEE	Sistema de Certificação Eletrónica do Estado
SGSSI	Secretário-Geral do Sistema de Segurança Interna
SIC	Sistemas de Informação e Comunicação

SIS	Serviço de Informações de Segurança
SSI	Sistema de Segurança Interna
UE27	UE a 27 países
UMIC	Unidade de Missão Inovação e Conhecimento
TIC	Tecnologias da Informação e Comunicação

Introdução

"Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots."

Sun Tzu, The Art of War (2009)

O mundo contemporâneo é distinto do de há dez ou 20 anos atrás, quando os computadores pessoais e as tecnologias de informação e comunicação (TIC) não estavam ainda vulgarizados e disseminados por toda a parte. A sua evolução exponencial até aos dias de hoje tornou possível um rápido desenvolvimento tecnológico, conducente a uma constante miniaturização dos componentes informáticos e a uma progressiva redução de custos, permitindo assim, que o que inicialmente se constituía como uma ferramenta de trabalho adquirida pelas empresas, se transformasse num instrumento lúdico e, mais tarde, num fenómeno social materializado através das inúmeras redes sociais existentes.

A par desta explosão tecnológica, assistimos também a um vertiginoso aumento da utilização da tecnologia e sistemas informáticos para comandar, controlar e monitorizar processos e sistemas em infraestruturas, como é o caso das redes de água, energia, telecomunicações e transporte, assim como no que concerne ao sistema financeiro, distribuição de água e mesmo, até, aos serviços de emergência nacional.

Esta dependência tecnológica, nomeadamente, a associada com as estruturas em rede que permitem a partilha de informação, conferindo capacidade de comando e controlo remoto entre diferentes pontos de um sistema, originou pontos de vulnerabilidade, sujeitos a ataques por parte de entidades que procuram, à margem da lei, obter dividendos ilícitos, informações confidenciais ou, simplesmente, perpetrar ataques à própria infraestrutura informática.

O ciberespaço não é algo que já existisse e que o homem tivesse aprendido a usufruir - à semelhança do mar, da terra, do ar ou do espaço - mas antes uma criação do próprio ser humano que como imperfeito que é, criou também um ambiente com falhas, que são aproveitadas para efetuar ciberataques. (Nunes, 2012a)

Para se delinear uma estratégia nacional de ciberdefesa, é necessário identificar quais são as nossas vulnerabilidades críticas, ou seja, o que queremos proteger e de que forma o poderemos fazer. Não será, pois, despiciendo o exercício académico de tentar

retirar ensinamentos dos ataques recentemente perpetrados contra certos países, como, por exemplo, a Estónia em 2007 (Anexo C).

Por outro lado, será também relevante perceber, não só como estão organizados outros países, para fazer face à ameaça de um ciberataque, mas também que estruturas e doutrinas foram desenvolvidas por estes nesse sentido, de forma a aproveitar todo um manancial concetual que possa já existir, e seguidamente, efetuar um exercício de *benchmarking*, que permita indicar caminhos possíveis para o nosso País, que garantam a sua eficaz proteção contra um eventual ciberataque.

As TIC têm uma importância fundamental para a sociedade e para a economia. Estas tecnologias, sendo seguras e de confiança, revestem-se de um grande valor para a prosperidade e bem-estar das sociedades, transformando-se num catalisador para um desenvolvimento económico sustentável. No entanto, estas tecnologias também aumentam a vulnerabilidade da sociedade ao fomentar a conceção de produtos e serviços que se tornam vitais. Uma disrupção deliberada ou não intencional, resultado de uma falha humana, técnica ou por causas naturais, pode originar distúrbios sociais. A complexidade das infraestruturas associadas às TIC e a nossa crescente dependência delas dão, assim, origem a novas vulnerabilidades (NCSS, 2011, p. 2).

Desenvolver e atualizar uma Estratégia Nacional de Ciberdefesa (ENC) é uma necessidade inerente à era da informação. Inúmeros países reviram recentemente os seus conceitos estratégicos no que toca à segurança das suas próprias sociedades de informação. À medida que as ciberameaças ganham relevo nos planos público e privado, torna-se necessário desenvolver esforços adicionais para estes dois setores. A falta de terminologia comum, de incentivos para o estabelecimento de parcerias público-privadas e os próprios custos associados com a cibersegurança são apenas alguns exemplos das preocupações suscitadas (Tikk, 2011a, p. 5).

Em Portugal, esta matéria está no centro das preocupações da tutela, como o demonstra a recente intervenção do Secretário de Estado Adjunto e da Defesa Nacional, Paulo Braga Lino, durante a abertura do Seminário Internacional "Ciberespaço e Estratégia Nacional de Informação", no Instituto de Defesa Nacional (IDN), em setembro de 2011 onde referiu que "as ameaças à segurança tanto se previnem e combatem no terreno, onde Portugal continua e continuará a garantir a sua presença, como no ciberespaço, onde importa mobilizar a capacidade e o conhecimento científico nacional". Continuou, afirmando que "a exploração, competitiva ou hostil, do ciberespaço pode ameaçar

processos de governação dos estados ou das empresas, sectores financeiros, industriais ou tecnológicos, serviços e infraestruturas de natureza estratégica sensível, em especial infraestruturas de informação que apoiam o exercício das funções de soberania do estado, designadamente, as Forças Armadas e as Forças de Segurança" (Lino, 2011, p. 4).

Assim, é propósito deste estudo contribuir para a identificação das capacidades desejáveis de cibersegurança e ciberdefesa a nível nacional, para fazer face à ameaça de um ciberataque. Para tal, elencaram-se como objetivos específicos: fazer um ponto de situação das atuais capacidades nacionais de ciberdefesa, determinando quais as medidas a desenvolver nesta matéria, considerando - numa perspetiva o mais abrangente possível - as diversas componentes envolvidas (doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade), circunscrevendo este esforço ao universo da Defesa Nacional e das Forças Armadas (FFAA).

Neste sentido, recorrendo ao método de investigação em ciências sociais proposto por Quivy e Campenhoudt (2005), foi identificada, como referência orientadora da investigação efetuada, a seguinte pergunta de partida:

"De que forma será necessário desenvolver as atuais capacidades de ciberdefesa nacionais, de forma a permitir uma eficaz cibersegurança relativamente às vulnerabilidades críticas da infraestrutura da informação?".

A pergunta de partida leva a duas perguntas derivadas:

PD1. *"Em que medida a atual capacidade de ciberdefesa nacional será eficaz para fazer face a um ciberataque?";*

PD2. *"De que forma será necessário desenvolver as capacidades de ciberdefesa nacionais para melhorar e complementar as existentes?".*

Na construção da problemática, indispensável ao estudo, o autor procurou romper com qualquer ideia preconcebida relativamente ao tema. Formularam-se, assim, as seguintes hipóteses, cuja validação será concretizada no desenvolvimento deste trabalho:

H1. *"A atual capacidade de ciberdefesa nacional é ineficaz para fazer face a um ciberataque.";*

H2. *"As capacidades de ciberdefesa nacionais terão de ser desenvolvidas de forma conjunta, combinada e integrada com as estruturas civis.".*

Com base em entrevistas e na consulta efetuada a publicações técnicas, revistas, livros, *sites* na internet e relatórios oficiais, tornou-se patente o caminho a seguir que

resultou no modelo de análise que se apresenta no Mapa Concetual do Apêndice 2, incluindo-se no Apêndice 1 o Corpo de Conceitos a este associado.

Este trabalho está organizado em três capítulos. No primeiro será efetuado o enquadramento estratégico e operacional deste tema, através duma análise às estruturas e capacidades nacionais, apurando as potencialidades e as vulnerabilidades existentes. No capítulo seguinte, procurar-se-á materializar uma abordagem comparativa, estudando determinadas organizações internacionais - identificadas como possíveis referências no que respeita à atuação no ciberespaço - que servirá como base para a análise das estratégias de ciberdefesa implementadas a nível internacional. Feito este levantamento, dedicar-se-á o terceiro e último capítulo à determinação das capacidades a desenvolver nacionalmente no âmbito da Defesa Nacional e das FFAA. Finalmente, apresentar-se-ão as conclusões gerais do trabalho e as recomendações consideradas pertinentes.

A cibersegurança e a ciberdefesa nacional e internacional, seja no âmbito militar, governamental ou privado, são matérias sensíveis e de cariz vital para os atores envolvidos. A informação necessária para escalpelizar os conceitos que serão apresentados, iria requerer um nível de credenciação elevado e em muitos casos não seria sequer disponibilizada. Assim, pretendendo manter o presente trabalho sem qualquer classificação de segurança, foram selecionados conteúdos de fonte aberta, não se incorrendo por conseguinte, no risco de comprometer informação sensível das entidades e organismos abordados nesta investigação.

Na referenciação bibliográfica deste trabalho recorreu-se ao *software* de referenciação incorporado no Microsoft Word, utilizando o estilo "Harvard-Anglia"[1], tal como previsto na NEP n.º 218 do IESM.

[1] Disponível em http://bibword.codeplex.com.

1. Capacidades de Ciberdefesa Nacionais

Em Portugal não está definida uma estratégia de cibersegurança. Não existem entidades primariamente responsáveis e formalmente mandatadas do ponto de vista legal, para exercer a coordenação de uma resposta concertada ao nível político, estratégico, ou militar. A Fundação para a Computação Científica Nacional (FCCN) é tida como referência e contato, funcionando o *Computer Emergency Response Team* (CERT) como um centro ao nível nacional, não possuindo, no entanto, um mandato do Governo para atuar sob o ponto de vista da coordenação de respostas nacionais no âmbito da cibersegurança.

Tal não significa que não exista qualquer tipo de segurança. Existe uma análise das infraestruturas críticas nacionais e das suas vulnerabilidades, por parte das entidades que são por elas responsáveis e que para o efeito desenvolveram mecanismos de proteção específicos, como é o caso da rede de emergência nacional, a rede das FFAA que está separada das outras redes ou da Portugal Telecom (PT). Nenhuma destas está, no entanto, mandatada pelo Estado para assegurar a segurança como um todo. O próprio Conceito Estratégico de Defesa Nacional (CEDN) é omisso na identificação das ciberameaças e do potencial disruptivo que possuem.

Exemplo recente das vulnerabilidades nacionais está patente nos repetidos ataques de piratas informáticos, ligados a um grupo intitulado LulzSec Portugal, quando estes fizeram com que diversos serviços da Polícia de Segurança Pública (PSP) ficassem inoperativos na noite de segunda-feira, dia 28 de novembro de 2011.

Os ataques deste grupo radical, alegadamente usados como retaliação pelas agressões sofridas durante a manifestação do dia 24 do mesmo mês em Lisboa, já atingiram outras instituições, tais como, o Hospital da Cruz Vermelha, o Portal das Finanças e o *site* do Parlamento, que esteve em baixo várias horas. No dia 29 de novembro de 2011, a PSP identificou diversas tentativas externas de intromissão no seu *site* institucional, as quais não haviam surtido efeito (Amaro, 2011).

Os ataques dos piratas informáticos, que já duram há alguns meses, já atingiram o Ministério da Administração Interna (MAI), o Serviço de Informações de Segurança (SIS), pelo menos três partidos políticos e a Rádio e Televisão Portuguesa. Os ataques causaram ainda danos no Sindicato Nacional da Carreira de Chefes da PSP tendo a sua página na internet sido modificada e copiada, e posteriormente difundida uma listagem com os

associados e respetivos contactos telefónicos. Este ato foi idêntico ao que culminou com a divulgação de dados pessoais de 107 polícias, ao serviço de três esquadras na zona de Chelas, no dia 27 de novembro de 2011 (Amaro, 2011).

Na opinião do TCor Viegas Nunes, deverá ser definida uma política de cibersegurança, assim como, uma estratégia para a sua implementação. O Conceito Estratégico de Defesa Nacional encontra-se em revisão, estando previsto que contemple a área da informação e da segurança do ciberespaço. Sendo esta uma área de soberania, o Estado não a deverá delegar. São urgentes orientações claras nesta matéria, pelo que caberá ao Estado - numa fase inicial - chamar a si esta responsabilidade. A fragilidade de todas as redes de informação nacional é bastante grande, existindo um problema de *outsourcing* da função de segurança da informação (Nunes, 2012a).

Importa pois, para melhor compreender a dimensão deste problema, fazer seguidamente, o levantamento das entidades, estruturas e organizações, que a nível nacional atuam no âmbito da cibersegurança, bem como caraterizar o contexto político-internacional em que o fazem, buscando encontrar a melhor forma de tirar partido das capacidades de ciberdefesa que já existem em Portugal.

a. Governamentais

Ao nível do Governo, no âmbito da segurança de materiais classificados, a Autoridade Nacional de Segurança (ANS) é a entidade responsável pela segurança dos sistemas informáticos, sendo as suas competências atribuídas, nomeadamente pelos SEGNACs 1 e 2, aprovados, respetivamente, pelas Resoluções 50/88, de 3 de dezembro, e 37/89, de 24 de outubro (Resolução do Conselho de Ministros n.º 5, 1990).

Na dependência da ANS está o Gabinete Nacional de Segurança (GNS) (Anexo A) que tem por missão: "garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais em que Portugal se insere, exercendo 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 Eletrónica do Estado (SCEE) - Infraestrutura de Chaves Públicas" (GNS, 2012).

No âmbito do SCEE funciona o Centro de Gestão da Rede Informática do Governo (CEGER) e a Entidade de Certificação Eletrónica do Estado (ECEE) na sua dependência. No anexo B encontra-se uma descrição sucinta destas entidades, assim como, um esquema

do Edifício de Segurança da Informação Nacional, em constante desenvolvimento, integrando as diversas componentes ou dimensões estratégicas da segurança.

O GNS tem como principais atribuições: "garantir a articulação e a harmonização dos procedimentos relativos à segurança da informação classificada em todos os serviços, organismos e entidades, públicos ou privados, onde seja administrada tal informação, designadamente e em especial, os da Administração Pública, das FFAA e das Forças e Serviços de Segurança, bem como, no âmbito das organizações, reuniões, programas, contratos, projetos e outras atividades internacionais em que Portugal participe".

Por outro lado, assegura: "nos termos dos instrumentos de vinculação do Estado Português, a proteção e a salvaguarda da informação classificada emanada das organizações internacionais de que Portugal faça parte ou das respetivas estruturas internas, nomeadamente no âmbito da Organização do Tratado do Atlântico Norte (OTAN) da União Europeia (UE), da Unidade Europeia de Cooperação Judiciária (EUROJUST) e da Agência Espacial Europeia (AEE), bem como de outros Estados com os quais tenham sido celebrados acordos de segurança" (GNS, 2012).

Sendo a Segurança e Defesa funções essenciais do Estado, segundo Alexandre Caldas, Diretor do CEGER, deverá ser o Estado - agente primordial na garantia do objetivo teleológico de segurança - a liderar e promover uma ENC, integrando-a na sua própria estratégia de *e-Government* e conduzindo-a como uma das suas ações executivas, num momento onde a proteção das Infraestruturas da Informação Críticas Nacionais (I2CN), se tornou não só numa necessidade, como um imperativo. A figura 1 apresenta a forma como a ação estratégica se deverá orientar, em termos da integração internacional (Caldas, 2011, pp. 94-95).

Figura 1 - Integração internacional da Estratégia Nacional de Cibersegurança.

Adaptado de Caldas (2011, p. 95).

A necessidade de um Centro Nacional de Cibersegurança (CNC) foi já identificada por várias entidades. Antero Luís, Secretário-geral do Sistema de Segurança Interna (SGSSI), considera necessária uma estratégia nacional "que não pode ser diferente da de outros países", que passa por dois níveis, um estratégico e outro tático. A dúvida é se deve ser criada uma nova estrutura ou aproveitar as já existentes, congregando os três Conselhos Superiores de Defesa, Administração Interna e de Informações. No geral, é preciso "agregar o que hoje anda disperso e que não se deixe ninguém de fora", referiu, salientando que se trata de "uma decisão política" necessária para "cimentar o que já existe" (Fonseca, 2011).

Na sua palestra no IESM no dia 30 de janeiro de 2012, Antero Luís referiu que o Sistema de Segurança Interna (SSI) poderia assumir as funções de entidade coordenadora da estratégia de cibersegurança nacional, enquanto facilitadora do diálogo entre as estruturas que a nível civil, governamental e militar desenvolvem esforços neste âmbito, à semelhança de outras áreas de segurança interna, permitindo otimizar recursos e evitar duplicação de tarefas. No entanto, refere que não teria capacidade para desempenhar funções de cariz técnico dada a dimensão reduzida do seu *staff*. Por fim, menciona a tendência existente de gerar este órgão coordenador na ANS (Luís, 2012).

Na sua conferência no IESM no dia oito de fevereiro de 2012, o TGen António Mascarenhas[2], referiu que neste momento foi já identificada a necessidade de um órgão que coordene e supervisione a cibersegurança a nível nacional e que esta responsabilidade recairia sobre a ANS (Mascarenhas, 2012).

b. Militares

Os Estados estão a substituir os convencionais soldados por técnicos especializados na internet, levando a uma mudança de paradigma, inerente à indissociabilidade dos ciberconflitos relativamente aos conflitos tradicionais. A consciencialização de que existe hoje em dia um novo vetor da guerra – a ciberguerra – juntamente com os tradicionais mar, terra, ar e espaço, deverá suscitar a obtenção de novas capacidades, que permita criar forças nesta vertente. Os atores que não desenvolvam esforços neste domínio serão suplantados pelos seus adversários, ficando em desvantagem face ao atual ambiente caracterizado por uma forte competição (Silva, 2010, pp. 19 - 20).

[2] Ex-Vice-Presidente do Conselho Nacional de Planeamento Civil de Emergência.

No seminário subordinado ao tema "Ciberespaço: Espaço Virtual, Mediático e Global" organizado pela Academia de Ciências de Lisboa, no dia 25 de janeiro de 2012, foi apresentado pelo TCor Viegas Nunes, um modelo genérico para uma possível organização e atribuição de responsabilidades, relativos à segurança e defesa do ciberespaço em Portugal. Assim, no âmbito da cibersegurança - entendida neste contexto como o conjunto de medidas desenvolvidas para enfrentar problemas de segurança específicos do ciberespaço - as forças de segurança ficariam responsáveis pelas áreas do cibercrime e do ciberativismo, e o SIS pelas relativas ao ciberterrorismo e à ciberespionagem.

No contexto do ciberespaço, às FFAA seria atribuída a incumbência da ciberdefesa. Todas estas diferentes entidades desenvolveriam na sua esfera de atuação, esforços para prevenir, detetar, defender e recuperar face a ciberataques. Sobranceiro aos dois grandes pilares da segurança e da defesa do ciberespaço ficaria um órgão coordenador denominado por "Conselho Nacional" (Nunes, 2012b).

Na Constituíção da República Portuguesa (CRP) encontramos bases legais que permitem consubstanciar este modelo. Assim, no número dois, do seu artigo 273.º, temos que: "A defesa nacional tem por objectivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações, contra qualquer agressão ou ameaça externas.", pelo que será possível estabelecer o paralelismo com o contexto do ciberespaço e verficar que caberá às FFAA o garante da ciberdefesa nacional.

Por outro lado, o mesmo diploma refere, no número um, do seu artigo 272.º, que: "A polícia tem por funções defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos.". Continuando no número três do mesmo artigo é referido que: "A prevenção dos crimes, incluindo a dos crimes contra a segurança do Estado, só pode fazer-se com observância das regras gerais sobre a polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos." (CRP, 2005).

Em Portugal, as FFAA apoiam-se em Sistemas de Informação e Comunicação (SIC) para assegurarem o cumprimento das missões que lhes são superiormente atribuídas. A informação de cariz operacional e administrativo - crítica para as suas missões e para o seu funcionamento - é armazenada, processada e transmitida através destes sistemas, razão pela qual a sua eficaz proteção se torna num requisito importante. Vejamos, então, de que forma atualmente se procura materializar esta preocupação no EMGFA e nos Ramos.

(1) EMGFA

A Divisão de Comunicações e Sistemas de Informação (DICSI) do EMGFA tem por missão apoiar as áreas de planeamento, direção e controlo dos sistemas de informação e tecnologias de informação e comunicação inerentes ao comando e controlo nas FFAA. Na área da cibersegurança é sua responsabilidade promover a implementação da política conjunta de segurança da informação, de forma a garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA (EMGFA, 2012).

Através da sua publicação PEMGFA/CSI/301 de 23 de setembro de 2008, estabelece-se a estrutura orgânica, normas e procedimentos para garantir a capacidade de resposta a incidentes de segurança informática das FFAA.

É necessário implementar e gerir medidas de segurança e desenvolver uma Capacidade de Resposta a Incidentes de Segurança Informática das FFAA (CRISI-FA)[3]. Segundo o PEMGFA / CSI / 301: "a implementação da CRISI-FA permitirá responder de forma concertada a incidentes de segurança informática, relacionados com atividades de software malicioso, atividades de utilizadores não autorizados, negação de serviços, ou outras ameaças/vulnerabilidades inerentes às Comunicações e Sistemas de Informação (CSI) ".

Esta capacidade utiliza de forma coordenada as valências existentes nos Ramos das FFAA e no EMGFA, disponibilizando serviços reativos, pró-ativos e de gestão de segurança e qualidade de serviço. Para a gestão e tratamento de incidentes de segurança informática dispõe ainda de um sistema de registo de incidentes, dum portal CRISI e de diversos equipamentos para o desempenho das suas funções. A estrutura da CRISI - assente no princípio da eficiência - procura obter uma resposta coordenada dos recursos existentes através de três níveis de atuação e coordenação: o primeiro através do Centro de Coordenação da CRISI, seguido do Grupo de Resposta a Incidentes de Segurança Informática (GRISI) e um terceiro e último nível composto pelas Autoridades de Segurança dos SIC (EMGFA, 2008, pp. 1-1 - 2-5).

[3] A CRISI é uma componente da área da *Information Assurance*.

(2) Ramos

No que concerne aos Ramos, não foi intenção do autor abordá-los de forma separada, já que, as questões relacionadas com o ciberespaço requerem, como se tem vindo a mostrar, um tratamento holístico.

Contudo, como uma das principais fontes deste trabalho foi um oficial português do exército de reconhecida competência na matéria, o autor entendeu por bem auscultar a sensibilidade de especialistas da Marinha e da Força Aérea neste domínio.

Se as ICN forem alvo de um ciberataque, quem pode e deve intervir são as FFAA, devendo estas possuir capacidades de ciberdefesa. Num momento em que assistimos à militarização do ciberespaço, com a criação por parte dos EUA de um cibercomando (CYBERCOM), em simultâneo com o desenvolvimento de capacidades de ciberdefesa militares por parte de outros países, Portugal e as suas FFAA deverão acompanhar este processo, evitando assim sair do "circulo de confiança" e como tal, de serem considerados neste âmbito. Assim, todos os Ramos deverão ter um sistema de cibersegurança na sua rede específica, com um centro de controlo e gestão de rede a ser coordenados pelo EMGFA (Nunes, 2012a).

No entanto, de acordo com o Trabalho de Investigação de Grupo realizado no âmbito do Curso de Estado-Maior do Exército no IESM, no ano letivo de 2011 - 2012, subordinado ao tema "*Cyberwar* – Definição, possibilidades de desenvolvimento de um modelo nacional de implementação*"*, as principais vulnerabilidades detetadas nas FFAA são a dispersão de meios, associada com a duplicação de estruturas e de capacidades similares de defesa e proteção em cada Ramo; a ausência de partilha de informação técnica ao nível das Equipas CIRC; a acumulação de funções dos militares, que origina uma proficiência abaixo do desejável; a ligação com entidades civis que deveria ser veiculada através de um único e representativo locutor das FFAA, de forma a permitir uma maior capacidade de influência e de consolidação da informação; e a Doutrina e terminologia não uniformizada entre os diferentes Ramos, que é concetualmente pouco detalhada nas publicações existentes (Morais, et al., 2011, p. 17).

Segundo o 1TEN STP Paulo Neves, do Gabinete de Engenharia de Sistemas do DITIC, atualmente a Marinha não possui ainda uma equipa dedicada para responder às questões de cibersegurança, estando numa fase final de preparação do estabelecimento de uma CRISI, num projeto que prevê desenvolver as capacidades de ciberdefesa, de forma faseada, num período de quatro a seis anos. Numa primeira fase, o esforço residirá na

prevenção, deteção, defesa e recuperação de incidentes que ocorram nos segmentos classificados da rede militar da Marinha, estendendo-se depois gradualmente à infraestrutura e serviços que apoiam a organização e a sua interligação com os outros Ramos, acabando por abranger todos os segmentos de rede e todos os serviços. Este projeto tem sido desenvolvido com a estreita ligação ao CERT.PT, nomeadamente no que se refere à plataforma de registo e acompanhamento dos incidentes *Request Tracker for Incident Response* (RTIR) (Neves, 2012).

Segundo o Tenente-Coronel Paulo Alves, chefe da Repartição da Segurança de Informação da Divisão de Comunicações e Sistemas de Informação do EMFA, perspetiva-se a criação de um CNC, que se constituirá como uma oportunidade para o estabelecimento de uma organização estruturada, com responsabilidades atribuídas, e na qual figurarão obrigatoriamente as FFAA. Não existe no entanto, até à data, documentação que formalize as responsabilidades, dependências e procedimentos de atuação a implementar, o que impede a atribuição de funções nas correspondentes áreas de atuação para as diferentes organizações relevantes para a cibersegurança nacional.

As preocupações da Força Aérea Portuguesa (FAP) prendem-se, quase exclusivamente, com a defesa de perímetro, isto é, com uma postura muito reativa. Nesse capítulo, possui *firewall,* inclusive aplicacionais, e *Intrusion Detection Systems* (IDS). No entanto, não é efetuado tratamento dos dados, isto é, a correlação dos eventos. Ou seja, só os ataques graves - como por exemplo ao *Domain Name System* (DNS) - podem ser detetados, uma vez que faltam informações relacionadas com esta análise, assim como, recursos humanos que possam ser afetados a esta função. Quanto à recuperação, são efetuados *back-ups* periódicos, apesar de este procedimento não estar vertido em norma. A FAP encontra-se representada na CC-CRISI, à semelhança dos outros Ramos, fazemos parte do fórum *Computer Security Incident Response Team* (CSIRT), dinamizado pela FCCN, e onde têm assento os *Internet Service Providers* (ISP), bancos, faculdades, entre outras entidades. A FAP participa ainda, à semelhança dos outros Ramos, em todas as reuniões, estatísticas e formações organizadas a nível nacional. A nível internacional participou ativamente e pela primeira vez no Cyber Coalition 2011, estando prevista a sua participação também na versão de 2012, encontrando-se esta em fase de preparação pelo CC-CRISI (Alves, 2012).

c. Civis

Na conferência no Instituto da Defesa Nacional subordinada ao tema *"Partnerships in Cyber Security"* no dia 14 de dezembro de 2011, o Brigadeiro-General Gregory L. Brundidge[4], ressalvou a importância das Parcerias Público-Privadas (PPP) e da integração das estruturas militares, públicas e privadas para a criação de uma estratégica eficaz de cibersegurança. Esta dimensão holística, resulta do novo e paradigmático mundo informático, que acaba por se relacionar com tudo e com todos em toda a parte, direta ou indiretamente.

Ainda segundo o General Brundidge, devemos primeiro "preocuparmo-nos com as necessidades do todo antes de nos consumirmos com as necessidades das partes", apresentando um modelo concetual para o relacionamento no seio das PPP, onde identifica a necessidade dos militares desenvolverem por um lado, doutrina em conjugação com as entidades públicas, e por outro, delinear estratégias com as organizações privadas. Por sua vez o setor público e o privado deverão contribuir com o desenvolvimento de programas que permitam melhorar as capacidades de ciberdefesa nacionais.

Dada a heterogeneidade destes atores, o General Brundidge identifica como principal desafio à capacidade de trabalhar em conjunto, para o mesmo estado final desejado, as diferentes culturais existentes e não a tecnologia. Para unificar este esforço colaborativo deverá, por último, ser definida regulamentação transversal a todos estes intervenientes. O setor privado possui a infraestrutura do ciberespaço, pelo que se torna essencial no desenvolvimento de uma estratégia de cibersegurança nacional. Mencionado também, como um ator importante no desenvolvimento das capacidades de ciberdefesa, são as instituições académicas (Brundidge, 2011).

Ainda na sequência da mesma conferência, Stephen Allen Ewell[5] elaborou sobre as linhas gerais que uma estratégia de cibersegurança deve ter para ser bem-sucedida. Assim, desde logo, esta deverá estar assente em dois pilares sólidos: um robusto relacionamento internacional e o livre fluxo de informação, ao que se associam os princípios de abertura, interoperabilidade, segurança e fiabilidade. Assim, a cooperação entre as nações aliadas

[4] Diretor de Comando, Controlo, Comunicações e Integração de Combate do Quartel General dos EUA na Europa, em Estugarda.
[5] Diretor Executivo da ECJ6 do Quartel General dos EUA na Europa, em Estugarda.

deverá compreender a partilha das capacidades de aviso prévio e de boas práticas identificadas, num esforço de desenvolvimento e de treino conjuntos.

Um dos desafios também apontado por Ewell ao desenvolvimento da cibersegurança, são as diferenças culturais que terão de ser vencidas, no sentido de permitir a harmonização da parceria entre Estado, FFAA e setor privado. Por fim, deverá ser estabelecida uma hierarquia de prioridades, no sentido de percecionar o que realmente é crítico e urge proteger, afirmando que "aquele que quer proteger tudo, acaba por não proteger nada" (Ewell, 2011).

Analisando algumas das ICN, poderemos constatar que quando a PT tinha o monopólio das comunicações, este era considerado um serviço público e esta tinha a obrigação de garantir a segurança desse serviço. A partir da liberalização das comunicações, a segurança passou a ser comercializada, tendo o utilizador de pagar mais pela mesma. Havendo políticas de segurança diferentes em cada empresa, cabe ao Estado - se estiver preocupado com a segurança da rede como um todo – a criação de mecanismos de fiscalização e o estabelecimento de um nível de segurança mínimo aceitável, que impeça a ocorrência de ataques massivos à rede (Nunes, 2012a).

É necessário o Estado criar um organismo com esta missão, sob pena de não termos um nível de segurança necessário para impedir a ocorrência de um ataque com consequências graves. As ICN dependem estruturalmente da eletricidade e funcionalmente dos sistemas de informação. A rede de distribuição de energia elétrica depende também funcionalmente dos sistemas de informação, pelo que desta constatação poderemos concluir, quanto à importância para o país, da necessidade de garantir a segurança dos sistemas de informação. O centro de gravidade do risco social, neste domínio, está nas redes de telecomunicações (Nunes, 2012a).

De acordo com a FCCN, os incidentes de grandes dimensões têm-se demonstrado críticos para atividades que abrangem todos os sectores da sociedade. Por outro lado, as tendências recentes mostram que os grandes incidentes de segurança das redes de informação, acontecem em infraestruturas profissionais e visam o ganho financeiro dos seus perpetradores. Os CSIRT são considerados essenciais na prevenção e reação a este tipo de fenómeno, juntamente com os serviços do CERT, que a nível nacional e internacional intervêm e coordenam a resposta a incidentes, assim como efetuam a divulgação e a promoção do conceito CSIRT no território nacional (FCCN, 2012).

Insurgentes que procurem pontos vulneráveis num determinado país irão certamente procurar vulnerabilidades na sua infraestrutura de informação, como aconteceu na Estónia em 2007 e na Geórgia em 2008 (Anexo C). Além de resiliente, qualquer estratégia de ciberdefesa deverá desenvolver parceiras com os aliados além-mar, assim como a nível doméstico (Watts, 2011).

Um ataque com um grau de severidade similar ao que sofreu a Estónia em 2007, não só é possível de ocorrer em Portugal, como deveria ser equacionado com objetividade. Portugal poderá não constituir um alvo interessante ou então a sorte tem pendido a favor do nosso país pelo facto de não termos sido ainda visados para um ataque deste género (Nunes, 2012a).

No decorrer do seminário subordinado ao tema "Ciberespaço: Espaço Virtual, Mediático e Global" organizado pela Academia de Ciências de Lisboa no dia 25 de janeiro de 2012, também o senhor professor doutor Luís Torres Magalhães, presidente da UMIC – Agência para a Sociedade do Conhecimento, IP , salientou a necessidade de uma intensa cooperação internacional, onde se estabeleça uma conjugação de forças, de forma a permitir uma eficiente ciberdefesa (Magalhães, 2012).

A segurança dos sistemas de informação continua a ser dirigida à proteção hermética e institucional das I2CN, não existindo uma estrutura integradora e normalizadora de âmbito nacional, dada a autonomia e por vezes desadequação com que os diferentes organismos implementam as suas políticas de segurança. A nível nacional não existem estruturas e doutrinas operacionais, vocacionadas para a condução de Operações de Informação defensivas de nível estratégico, pelo que a estrutura existente não se revela adequada para garantir a proteção das I2CN, num ambiente de informação caraterizado por novas ameaças e riscos (Nunes, 2009, p. 14).

Os indicadores recolhidos até esta fase da investigação, apontam para existência de um esforço nacional a nível da ciberdefesa e da cibersegurança, englobando os setores governamental, civil e militar, mas que no entanto, evidencia pouca articulação e coordenação destes atores essênciais da sociedade de informação - até mesmo dentro dos Ramos das FFAA - que apresentam ainda diversas vulnerabilidades e dificuldades de integração concetual e operacional. Para as deficiências apontadas neste trabalho contribui a falta de uma estratégia nacional de ciberdefesa, contendo uma entidade coordenadora e mandatada para harmonizar e gerar as sinergias necessárias, para alcançar o desiderato da efetiva capacidade de prevenção, deteção, defesa e recuperação contra um ciberataque, que

permita a proteção das ICN e das I2CN. Assim, foi possível responder à primeira pergunta derivada *"Em que medida a atual capacidade de ciberdefesa nacional será eficaz para fazer face a um ciberataque?"* ao validar a primeira hipótese formulada: *"A atual capacidade de ciberdefesa nacional é ineficaz para fazer face a um ciberataque."*.

As capacidades de ciberdefesa nacionais, com enfoque na proteção das ICN, deverão agilizar o seu campo de atuação com as diversas entidades internacionais, que a nível das diferentes redes de informação e de conhecimento em que Portugal se insere - nas esferas política, comercial, militar e académica - permitem a ligação com o mundo, na procura da satisfação dos nossos interesses superiores.

A compreensão do caminho percorrido pelas agências, organizações, institutos e até mesmo países, que se constituem como nós desta rede global de informação, veiculada pela internet, poderão dar indícios que permitam fomentar uma estratégia nacional de ciberdefesa, que não esteja apenas voltada para o seu interior, mas que procure uma abordagem holística e global desta nova realidade e dimensão.

No próximo capítulo será efetuado uma análise às capacidades internacionais no âmbito da ciberdefesa, criando o enquadramento basilar para a conceptualização que será efetuada no terceiro capítulo, procurando desta forma percecionar o estado da arte a nível internacional, e recolher indicadores que permitam concluir quanto a uma estratégia nacional de ciberdefesa.

2. Capacidades de Ciberdefesa das Organizações Internacionais

A perceção global sobre as ciberameaças mudou drasticamente depois dos ciberataques ao governo da Estónia em 2007. Patente ficou o preço a pagar por se ter uma sociedade de informação avançada, quando motivações políticas e ideológicas originaram um ciberataque sem precedentes às infraestruturas críticas daquele país, servindo em simultâneo como chamada de atenção para especialistas informáticos de todo o mundo, para as graves consequências associadas. Casos mais recentes como o *worm*[6] que atacava o *Microsoft Windows*[7] e os ciberataques contra o *Google* na China em 2010[8], mostram o grau crescente de sofisticação do cibercrime (Tikk, 2011a, p. 2).

Antes do incidente na Estónia, as organizações tendiam a tratar isoladamente os riscos com que lidavam. Neste quadro, a cibersegurança era apenas a soma dos planos individuais de contingência, não atendendo às ameaças sistémicas e que transversalmente visavam todas estas entidades, resumindo-se ao desenvolvimento de soluções estandardizadas, em vez de conceberem planos ou capacidades para encetar ações coordenadas. No entanto, desde 2007, a ONU, a UE e a OTAN, entre outras organizações internacionais, introduziram novas políticas de cibersegurança ou reviram as antigas. Também no plano legal houve necessidade de adaptação às novas ameaças, uma vez que estas põem à prova os limites da legislação existente, sobre proteção da informação, comunicações eletrónicas e de acesso às informações públicas (Tikk, 2011a, pp. 2-3).

Vejamos de seguida, como a OTAN tem vindo a desenvolver as suas capacidades de ciberdefesa, assim como, o esforço desenvolvido pelo seu centro de excelência para a ciberdefesa na Estónia.

a. Organização do Tratado do Atlântico Norte

No final de 1990, a OTAN sofreu uma série de ciberataques que chamaram a sua atenção para este novo domínio da conflitualidade, quando *hackers* pró-sérvios atacaram *sites* da internet da OTAN. Durante o conflito no Kosovo, o *site* da OTAN ficou muitas vezes inoperativo devido a ataques do tipo *Directed Denial of Servive* (DDoS). Durante a Cimeira de

[6] Um *worm* (verme, em português) é um programa autorreplicante, semelhante a um vírus, mas que ao contrário deste último é completo e não precisa de outro (programa) para se propagar (Webopedia, 2012).
[7] Ciberameaça conhecido por *Conficker*.
[8] Ciberataque conhecido por *Aurora*.

Praga de 2002, a OTAN criou um órgão, o *NATO Computer Incident Response Capability* (NCIRC), que tem sido capaz de detetar e impedir vírus informáticos e intrusões nos sistemas da OTAN, e providenciar nesta matéria, apoio aos seus aliados, com suporte doutrinário e forense (Kempf, 2011).

Segundo Suleyman Anil - chefe da ciberdefesa da OTAN - esta organização tem desenvolvido desde 2006, capacidades operacionais de defesa e criado um bom modelo de implantação e de exploração de tecnologias e capacidades de ciberdefesa. Na sua opinião, os governos não serão capazes, sozinhos, de responder às ciberameaças, pelo que importa desenvolver e melhorar as tecnologias neste âmbito. Deste modo, a partilha de informações e de conhecimento com o setor privado, poderá e deverá continuar a ser melhorada (Anil, 2011).

O *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCoE) foi formalmente criado no dia 14 de maio de 2008, a fim de reforçar a capacidade de ciberdefesa da OTAN. Localizado em Tallinn, na Estónia, a sua criação resulta do esforço internacional da Estónia, Letónia, Lituânia, Alemanha, Hungria, Itália, Polónia, Eslováquia, Espanha e EUA. O Centro recebeu a sua acreditação plena, no seio da OTAN, no dia 28 de outubro de 2008, atingindo o estatuto de organização militar internacional. A sua missão é melhorar as capacidades de cooperação e partilha de informação no seio da OTAN, e entre esta e os seus parceiros no âmbito da ciberdefesa, através da educação, investigação, desenvolvimento, partilha de lições aprendidas e de consultoria.

A visão do CCDCoE é ser a principal fonte consolidada de experiência na área da ciberdefesa cooperativa, através da acumulação, criação e disseminação de conhecimento no âmbito da OTAN e dos seus parceiros. Procurando acompanhar a evolução das tecnologias das comunicações, o CCDCoE tornou-se num dos mais avançados centros de pesquisa sobre ciberdefesa do mundo. No domínio da ciberdefesa cooperativa, o centro possuí um núcleo de pesquisa para as áreas Política e Legal; Conceitos e Estratégias; Ambiente Tático; e Proteção das I2CN (CCDCOE, 2011).

Em 2010, o *Allied Command Transformation* (ACT) definiu o *Framework for Collaborative Interaction* (FFCI), que permite à OTAN e às empresas privadas trabalhar em conjunto. Estas empresas privadas de cibersegurança foram convidadas para participar em eventos OTAN relacionados com a cibersegurança, tal como o *Information Assurance 2011 Symposium*, onde os diferentes palestrantes compartilham os seus conhecimentos com mais de 800 delegados de diferentes países da OTAN. Sem a cooperação com a

indústria privada, as redes da Aliança estariam quase certamente comprometidas (OTAN, 2011a).

Em junho de 2011, os Ministros da Defesa da OTAN adotaram uma nova política de ciberdefesa - seguindo as orientações do novo Conceito Estratégico - e que preconiza uma abordagem coordenada para a Aliança neste domínio, com foco na prevenção de ciberameaças e no aumento da resistência aos ciberataques, prevendo uma proteção centralizada de todas as estruturas da OTAN.

A política em apreço prevê a criação de mecanismos políticos e operacionais de resposta aos ciberataques por parte da OTAN, integrando a ciberdefesa no seu Processo de Planeamento de Defesa. Estabelece ainda os princípios de cooperação da OTAN - no âmbito da ciberdefesa - com os seus parceiros, organizações internacionais, o setor privado e ainda com as universidades. Paralelamente, foi desenvolvido um Plano de Ação de Ciberdefesa que servirá como ferramenta para garantir a aplicação oportuna e eficaz da nova política (OTAN, 2011b).

Também a UE possui - em complementaridade com a OTAN - diversos organismos que contribuem para a segurança dos seus Estados-Membros, protegendo informação vital veiculada entre estes, fruto das relações estabelecidas em áreas como a economia, segurança e defesa ou a investigação científica. Vejamos, de seguida, os principais organismos que a UE comporta, no domínio da cibersegurança e ciberdefesa, e que são elucidativos da crescente preocupação comunitária com as ciberameaças em particular e com o cibercrime em geral.

b. União Europeia

Em dezembro de 2005, o Conselho Europeu de Justiça e dos Assuntos Internos incumbiu a Comissão Europeia de apresentar uma proposta de criação de um Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC). O programa visa não só dar resposta à ameaça terrorista, mas também às atividades criminosas, riscos naturais e outras causas de acidentes, utilizando uma abordagem holística, centrando-se na proteção das infraestruturas com uma dimensão transnacional. O PEPIC foi assim criado com o objetivo de identificar as ICN, analisando as vulnerabilidades e interdependências existentes, e avançando com soluções para as proteger.

O programa contempla também o apoio aos setores industriais para a deteção das ameaças terroristas. Os corpos policiais dos países da UE e os serviços de proteção civil

devem garantir que o PEPIC faz parte integrante do seu planeamento e das suas ações de sensibilização (UE, 2010).

A nível nacional, a Lei n.º 62/2011, de 9 de maio, estabelece os procedimentos de identificação e de proteção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes, transpondo a Diretiva n.º 2008/114/CE, do Conselho, de 8 de Dezembro. Com este decreto-lei, estabelecem-se procedimentos para a identificação das diferentes infraestruturas com funções essenciais para a sociedade, cuja perturbação ou destruição teria um impacto significativo, ao inibir essas funções. Os procedimentos de identificação e de designação das Infraestruturas Críticas Europeias (ICE) aplicam-se ao sector da energia[9] e ao sector dos transportes[10] (MDN, 2011).

O esforço que a UE desenvolve a nível internacional, neste domínio, está patente na sua relação com os EUA. A comissão europeia através do seu projeto-piloto intitulado *"Transatlantic Methods for Handling Global Challenges in the European Union and United States"*, pretendeu avaliar o estado atual da segurança da UE e dos EUA, produzindo recomendações sobre o seu relacionamento, procurando fornecer aos responsáveis políticos europeus e norte-americanos, ideias e ferramentas que melhorem e aprofundem o diálogo transatlântico sobre questões de segurança comuns, para a UE e para os Estados Unidos, e identificar potenciais convergências transatlânticas.

No âmbito da cibersegurança foi recomendado que a coordenação e treino operacional, entre os EUA e a UE, fossem melhorados através da partilha de definições e conceitos partilhados e da criação de estruturas de cooperação no domínio da ciberdefesa, que fomentem um intercâmbio de lições aprendidas e boas práticas (Conley et al., 2011, pp. 1-6).

Segundo Federica Di Camillo e Valérie Miranda (2011, pp. 9 - 10), do *Istituto Affari Internazionali* de Roma, os ciberataques são uma ameaça crescente para os governos devido à natureza transnacional e interligada das I2CN. Apesar das questões relacionadas com o ciberespaço terem estado pouco presentes na retórica da UE, torna-se possível identificar uma consciencialização crescente do imediatismo das ciberameaças, refletido na

[9] Tais como infraestruturas e instalações de produção e de transporte de eletricidade; Infraestruturas de produção, refinação, tratamento, armazenagem e transporte, de petróleo por oleodutos e de gás por gasodutos e terminais para gás natural em estado líquido.

[10] Designadamente: Transportes rodoviários, ferroviários e aéreos; Transportes por vias navegáveis interiores; Transportes marítimos, incluindo os de curta distância, e portos.

criação de agências dedicadas e nos compromissos assumidos pela Comissão Europeia. A aproximação da UE à cibersegurança, passa por um quadruplo vetor que engloba medidas de segurança da informação, proteção das I2CN, combate ao cibercrime e a elaboração de um quadro legal que regulamente as comunicações eletrónicas, incluindo proteção de dados e da privacidade.

Nos Estados Unidos, a cibersegurança surge como uma prioridade de segurança nacional. Os esforços deste país neste domínio têm sido no sentido de fazer a ponte entre as historicamente separadas missões de ciberdefesa, com a aplicação da legislação, de informações e da contrainformação.

O governo dos EUA tem enveredado esforços no sentido de reforçar a cooperação entre as suas agências e departamentos, bem como com o setor privado, nomeadamente, com a base industrial de defesa e com as infraestruturas críticas visadas, de forma a melhor identificar as ciberameaças.

Apesar das aproximações da UE e dos EUA à cibersegurança terem muito em comum, a cooperação transatlântica necessita ser melhorada. Assim, no sentido de alcançar uma harmonização legislativa, deverá primeiramente ser conseguida uma concordância conceitual e semântica das questões relacionadas com o ciberespaço. Por outro lado, deverá ser dada uma maior prioridade e atenção à cibersegurança na agenda transatlântica, inclusivamente criando um Conselho de Cibersegurança UE-EUA, na mesma linha do Conselho da Energia existente entre estes.

Por último, deverá ser promovida a cooperação transatlântica ao nível operacional, através da criação de exercícios conjuntos e intercâmbios entre as agências dos EUA e da UE, incentivando a troca de boas práticas entre os seus CERT (Miranda et al., 2011, pp. 9 - 10).

Como exemplo das preocupações da UE, o Regulamento da Comunidade Europeia 460/2004, de dez de março, emanado do Parlamento e do Conselho Europeu, criou a *European Network Information and Security Agency* (ENISA). As operações desta agência começaram em Creta, em setembro de 2005, após um período de instalação inicial em Bruxelas. A ENISA auxilia a Comissão Europeia, os Estados-Membros e a comunidade empresarial, a lidar, responder e especialmente, a evitar problemas de segurança de rede e da informação. A ENISA constitui-se como um corpo de conhecimentos, criado pela UE, para realizar técnicas específicas e tarefas científicas no campo da Segurança da Informação. A agência também assiste a Comissão Europeia nos trabalhos técnicos

preparatórios, para a atualização e desenvolvimento da legislação comunitária, no domínio da segurança das redes e da informação, sendo portanto, a sua missão essencial para alcançar um nível elevado e efetivo de segurança na UE, neste domínio. Juntamente com as instituições da UE e os Estados Membros, a ENISA procura desenvolver uma cultura de segurança para o benefício dos cidadãos, consumidores, empresas e organizações do sector público na UE (ENISA, 2012).

Concluída a análise às capacidades nacionais e internacionais de ciberdefesa e cibersegurança, abordaremos de seguida as estratégias internacionais implementadas neste domínio e que se consideram de relevo para os objetivos deste trabalho. Este último capítulo proporcionará o contributo necessário para responder à pergunta de partida, possibilitando a elaboração de uma proposta de desenvolvimento das capacidades de ciberdefesa e cibersegurança, no âmbito da Defesa Nacional e das FFAA.

A análise efetuada até esta fase da investigação, patente nos indicadores recolhidos e apresentados, revela não só o esforço dedicado pela comunidade internacional, mas também a necessidade identificada de coordenar e estimular a cooperação interna, entre o setor privado e público, assim como, no plano externo, da criação de parcerias multinacionais que fomentem o desenvolvimento de capacidades de ciberdefesa, como são exemplo a UE e os EUA, ou a OTAN através do seu CCDCoE. Desta forma, foi possível responder à segunda pergunta derivada "De que forma será necessário desenvolver as capacidades de ciberdefesa nacionais para melhorar e complementar as existentes?" ao validar a segunda hipótese formulada "As capacidades de ciberdefesa nacionais terão de ser desenvolvidas de forma conjunta, combinada e integrada com as estruturas civis.".

3. Desenvolvimento das Capacidades Nacionais de Ciberdefesa

A comunidade internacional tem vindo, como demonstrado anteriormente, a tomar consciência de toda a problemática associada com um potencial ciberataque. Neste sentido, diversos países têm desenvolvido estratégias de ciberdefesa que permitam a geração de sinergias a nível nacional e também internacional, procurando criar parcerias no desenvolvimento de novas capacidades de ciberdefesa. Estas estratégias comportam-se como seres vivos em constante crescimento e mudança, procurando ajustar-se às mudanças do meio onde se inserem, de forma a assegurarem a sua sobrevivência.

Assim, a análise efetuada às estratégias de cibersegurança da Holanda, Estónia e dos EUA, permitiu a criação de uma imagem de conjunto, verificando os pontos comuns nas diversas visões e abordagens que permitem a ligação à questão central desta investigação, possibilitando desta forma ao autor, apresentar a proposta de capacidades a desenvolver no nosso país neste domínio.

De acordo com a *Research and Technology Organization* da OTAN, patente no seu *Technical Report* TR-071-06, o acrónimo composto pelos termos Doutrina, Organização, Treino, Material, Liderança, Pessoal e Infraestruturas (DOTMLPI) considerou-se conter os componentes necessários para definir uma capacidade. Indo de encontro ao enunciado proposto para a elaboração desta investigação, o autor, para efeitos da realização do presente trabalho, adotou também esta definição. No entanto, tal como previsto no mesmo *Tecnhical Report*, estas sete componentes não devem ser analisadas isoladamente, uma vez que cada uma delas tem capacidade para influenciar as outras. Por outro lado, existem áreas de sobreposição e semelhança entre estas, o que as permite agrupar e desta forma originar um acrónimo mais simples e percetível.

Atendendo a este conceito, considerar-se-á isoladamente a componente Doutrina (D), e agrupar-se-ão as restantes, duas a duas, da seguinte forma: o Treino e a Liderança em "T" de treino e a Organização e Pessoal em "O" de organização. Por fim, Material e a Interoperabilidade estarão vertidos em "I" de infraestrutura. Assim, será adotado o acrónimo DOTI, composto pela Doutrina, Organização, Treino e Infraestrutura para delimitar o conceito de capacidade a desenvolver neste capítulo (OTAN, 2006).

Usando os indicadores já apresentados neste trabalho e que permitiram responder às duas perguntas derivadas, através da validação das duas hipóteses associadas, irá efetuar-se

seguidamente, uma análise complementar e mais específica, às estratégias de ciberdefesa dos países selecionados e que permitirá responder à pergunta de partida da investigação.

a. Doutrina

A era da informação coloca aos Estados inúmeras dificuldades e desafios. Proteger a sociedade de ameaças assimétricas e que visam as ICN - cada vez mais dependentes das I2CN - e que se constituem como a base operacional para indústrias, organizações e para a própria economia, é um desiderato complexo. Esta dependência tem uma componente de segurança nacional vincada, uma vez que a infraestrutura da informação tem a dupla capacidade de permitir, por um lado, a vitalidade econômica do país, e por outro, a condução de operações militares e das atividades governamentais, especialmente dependentes dos provedores de telecomunicações, para toda uma panóplia de funções, tais como, logística e transporte. As tendências atuais, como a abertura e liberalização dos mercados e a globalização, estimuladores da interação transnacional, assim como do acesso generalizado às redes de telecomunicações, estão a elevar os requisitos de segurança das I2CN em todo o mundo (Krishna-Hensel, et al., 2007, pp. 152 - 155).

A doutrina deverá na opinião do autor, ser desenvolvida tendo em atenção a atual corrente da UE e da OTAN neste domínio, para que na sua génese não haja lugar a incompatibilidades, especialmente na componente militar, que terá do ponto de vista da complexidade e sensibilidade da informação veiculada, desafios acrescidos. Deverá incluir, geneticamente a componente governamental, civil e militar, procurando identificar as principais vulnerabilidades da I2CN e integrar a visão politico-estratégica na sua conceção, estabelecendo os níveis de ambição pretendidos e o esforço requerido a nível nacional.

O nível de ambição deverá ser ajustado às nossas potencialidades e ter em conta as nossas fraquezas e limitações. No entanto, deverá definir-se claramente se a meta a atingir fica pela mera proteção[11], ou se esta é uma das condições a estabelecer, para atingir outro patamar mais elevado e que passará pela superioridade da informação e que nos irá permitir enquanto país, desenvolver capacidades no domínio do ciberespaço, que reduzam o nosso Ciclo de Boyd[12] e nos permita usar a informação de forma mais proveitosa.

[11] Associada a uma das vertentes do conceito de Salvaguarda da Informação (*Information Assurance*), prevista no PEMGFA/CSI/301, de 23 de Setembro de 2008.
[12] Criado por John Boyd da Força Aérea norte-americana e representado num ciclo fechado de Observação, Orientação, Decisão e Ação.

De acordo com o MGen Aires, chefe da DICSI/EMGFA, a confiança na informação e nas TIC que a suportam, é fundamental para a tomada de decisão, tomando este desiderato especial importância quando as informações em questão, são respeitantes à ordem de batalha inimiga e servem como base para o exercício de C2 e para a processo de decisão, associado com o emprego de forças de combate (Aires, 2012).

Vejamos, de seguida, de que forma poderemos utilizar a experiência recente de alguns países proeminentes no domínio da cibersegurança e que consolidaram as suas estratégias nacionais de ciberdefesa, procurando assim, utilizar este conhecimento para o desenvolvimento das nossas capacidades nacionais.

(1) Holanda

De acordo com a estratégia de cibersegurança implementada pelo governo holandês, investir em cibersegurança significa investir no futuro, no crescimento económico e na inovação, possibilitando assegurar a utilização segura das TIC. Para atingir este desiderato torna-se necessário atribuir uma elevada prioridade à cibersegurança, nas suas vertentes civil-militar, público-privado e nacional-internacional, através de infraestruturas das TIC resilientes, em setores vitais resistentes, capazes de responder de forma efetiva e célere, e assegurando uma proteção legal adequada no domínio digital (NCSS, 2011, p. 3).

A visão holandesa sobre a cibersegurança é clara e simples: "Segurança e confiança numa sociedade de informação aberta e livre" e tem como objetivo aumentar a confiança dos seus cidadãos, da comunidade empresarial e do governo, na utilização das TIC. A Holanda reconhece que uma abordagem coerente e integral à questão da cibersegurança, passa por um empreendimento conjunto e orientado para redes, envolvendo a comunidade empresarial e instituições de conhecimento e investigação. Para tal, decidiu criar um Concelho de Cibersegurança, onde os representantes das partes relevantes terão uma posição de nível estratégico e no qual serão estabelecidos os requisitos para a elaboração e implementação da estratégia de cibersegurança.

Por outro lado, prevê a criação de um CNC, onde o setor público e o privado poderão contribuir com as suas experiências e conhecimento, permitindo uma maior consciência situacional dos novos desenvolvimentos, novas ameaças e tendências, que possam contribuir para a resposta a incidentes e para a tomada de decisão (NCSS, 2011, pp. 4 - 5).

(2) Estónia

Procurando nas recentes medidas previstas pela estratégia de cibersegurança da Estónia, podemos adicionalmente considerar na elaboração da nossa própria doutrina nacional de cibersegurança a definição de requisitos mais robustos de proteção das I2CN, das ICN e dos seus sistemas de controlo, de forma a aumentar a sua própria resiliência e a dos organismos associados, contras as ciberameaças. Sendo a segurança da internet vital para assegurar a cibersegurança, a sua infraestrutura física e lógica nacional deverá ser igualmente reforçada, assim como, promover o aumento de métodos mais eficazes de autenticação (Tikk, 2011a).

(3) EUA

O conceito de ligação das operações militares com o ciberespaço, denominado por alguns autores de "militarização do ciberespaço", tem como grande marco a criação do *Cybercommand* (CYBERCOM) pelos EUA. A sua missão é planear, coordenar, integrar, sincronizar e dirigir as operações de defesa das redes de informação, especificadas pelo Departamento de Defesa, preparando-se para conduzir todo o espectro de missões militares, de forma a assegurar a liberdade de ação das forças dos EUA e dos seus Aliados no ciberespaço, negando o seu uso aos adversários (DoD, 2010).

Os EUA, na sua revisão à doutrina do ciberespaço em 2009 e publicada no *site* institucional da Casa Branca, identificam a necessidade de uma forte ligação entre o setor público e privado, na partilha de responsabilidades em assegurar a segurança e fiabilidade da I2CN. Reconhece ainda que o seu governo deverá articular e coordenar os objetivos da sua infraestrutura de informação e comunicação, através de parcerias entre os dois setores da sociedade, público e privado.

Por outro lado, o governo deverá trabalhar com os principais interessados a nível nacional, para desenvolver a doutrina e os mecanismos que permitam mitigar as vulnerabilidades e possibilitem a tomada de decisão face a incidentes no ciberespaço (WhiteHouse, 2009, pp. 15 - 17). Também no nosso país este será o caminho a percorrer, e que permitirá a criação de raiz de uma verdadeira doutrina de cibersegurança e ciberdefesa nacional, integradora e aglutinadora dos vários níveis da sociedade, assente em bases sólidas, de forma a eliminar lacunas e espaços por onde códigos maliciosos e eventuais adversários possam explorar as nossas vulnerabilidades. Para tal, urge a criação de um

CNC que permita o diálogo e uma análise de conjunto da atual situação nacional e internacional, relativa ao ciberespaço e às ciberameaças.

(4) Portugal

Não existe a nível nacional uma estratégia de cibersegurança que englobe a vertente governamental com a civil e a militar, como ficou demonstrado pelos indicadores já apresentados. No entanto, foram dados recentemente passos importantes no sentido de colmatar as lacunas a nível doutrinário.

No decorrer do seminário subordinado ao tema "Ciberespaço: Espaço Virtual, Mediático e Global" organizado pela Academia de Ciências de Lisboa no dia 25 de janeiro de 2012, o Doutor Jorge Bacelar Gouveia, identificou a perda de três presupostos legais quando nos referimos ao ciberespaço. Assim, temos a perda de presencialidade, da territorialidade, a desmaterialização documental e do valor jurídico associado. Continua ainda, afirmando que o direito do ciberespaço se associa a todas as atividades humanas e que existe a necessidade de o adaptar a esta nova realidade, como por exemplo na celebração de um contrato, na tributação eletrónica, no direito inteletual, no direito constitucional[13], no voto eletrónico, e ainda na questão de punir quem prevarica neste domínio. Existe pois um campo vasto de adaptação às necessidades próprias do ciberespaço (Gouveia, 2012).

Na sua intervenção no Ministério da Administração Interna, no dia 16 de fevereiro de 2012, subordinada ao tema "O Desafio da Cibersegurança", o Ministro da Administração Interna, Miguel Macedo, afirmou que Portugal acompanhou a doutrina internacional e integrou o normativo europeu na sua ordem interna, através da Lei do Cibercrime[14] (nº 109/2009, de 15 de Setembro). Na sua opinião, uma política de cibersegurança deverá estruturar-se em quatro vetores de atuação:

(1) Garantir a segurança e confidencialidade da infraestrutura das TIC;

(2) Definir estratégias e políticas de segurança assentes na análise e gestão de risco;

[13] Como recolha de assinaturas para petições eletrónicas.

[14] Consciente da necessidade de regulamentar o uso indevido do ciberespaço, a Assembleia da República aprovou em 15 de setembro de 2009, a Lei n.º 109/2009, denominada Lei do Cibercrime, adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Esta lei estabelece as disposições penais materiais, tais como, danos relativos a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo ou interceções ilegítimas. Identifica ainda a responsabilidade penal das pessoas coletivas e entidades equiparadas, e estabelece diversas premissas relativas à cooperação internacional (AR, 2009).

(3) Alinhar e integrar operacionalmente as organizações, no equilíbrio necessário entre o direito à privacidade e a necessidade de acesso à informação, por parte das Forças e Serviços de Segurança, em nome da defesa e da segurança;

(4) Criar uma relação de parceria entre o sector público e o sector privado, em moldes aceites por todos, a funcionar em rede e de forma desburocratizada.

Considerou ainda, que se torna necessário assegurar a partilha e a disseminação de informação sobre ciberameaças, incorporar capacidades de reação adequadas ao cibercrime e estruturar a formação técnica neste domínio, em coordenação com escolas e centros de conhecimento especializados (Macedo, 2012).

A implementação de uma Estratégia Nacional de Segurança da Informação (ENSI), está prevista para fevereiro de 2013. A decisão de implementação da ENSI vem no seguimento das conclusões do Grupo de Projeto para as Tecnologias da Informação e Comunicação (GPTIC) e passará, entre outras medidas, pela criação de um CNC e pela revisão do quadro legal existente sobre informação classificada, ou seja, dos atuais SEGNAC's (Macedo, 2012).

Apesar dos esforços do GPTIC, a principal tónica das Resoluções do Conselho de Ministros n.º 46/2011 e n.º 12/2012 está na redução de custos associados com as TIC a nível nacional, tendo sido, no dia 10 de abril de 2012, realizada no auditório do Ministério da Defesa Nacional (MDN), a primeira reunião sobre o plano global estratégico de racionalização e redução de custos com as TIC na Administração Pública[15].

A posição defendida pelo MGen / DICSI foi a de que a criticidade da plataforma tecnológica de comunicações que serve as FFAA, sendo um elemento fundamental e crítico para sua capacidade de C2, deverá ficar fora deste plano de redução de custos. Por outro lado, as FFAA constituem-se como parte interessada na melhoria da eficiência, pelo que, pegando nestas duas vertentes, as FFAA deveriam ter um representante no GPTIC, o que não acontece.

Esta abordagem do MGen / DICSI foi corroborada pelos representantes dos Ramos das FA, tendo o representante da Marinha referido que faria sentido que os Ministérios relacionados com a Soberania Nacional (MDN, MAI, MNE e Justiça), nas áreas que não

[15] Entidades presentes na reunião: MDN/SG: Secretário-Geral, Dr. Gustavo Madeira/Secretário-Geral adjunto, CALM Carmo Durão/TC Colaço; EMGFA/DICSI: MGEN Aires/CMG Félix Marques; Marinha: CALM Gameiro Marques/CMG Alves Francisco/CFR Pereira Simões; Exército: MGEN Matias; Força Aérea: COR Figueiredo/COR Palha; Outros responsáveis das SI/TIC de vários organismos da área do MDN.

são transversais a toda a Administração Pública, ficassem excecionados da resolução em apreço. Na opinião do Secretário-Geral do MDN, a especificidades do MDN e concretamente das FFAA, na vertente das capacidades de comando e controlo, não deveria ficar abrangido pela Resolução de Conselho de Ministros n.º 12/2012, e que o Ministro da Defesa iria em sede de Conselho de Ministros pugnar por este objetivo (Aires, 2012).

Outra necessidade que advém em termos doutrinários e que está pouco explorado a nível nacional é a definição das Regras de Empenhamento (RoE), para os agentes que eventualmente serão mandatados e capacitados com o uso da força. Como defendido anteriormente neste trabalho, aos militares caberia esta capacidade. Um ciberataque por parte de um inimigo agindo contra a soberania nacional, obteria a mesma resposta militar, como se de um ataque armado por parte deste se tratasse. Ainda que polémico, o conceito subjacente é o de que uma ameaça ao nosso país, grave o suficiente para originar uma resposta cinética por parte das nossas FFAA, com o objetivo de cessar o ato hostil em curso, seria independentemente da forma de atuação do opositor.

Isto é, se um ciberataque às ICN, provocando um efeito disruptivo a nível das telecomunicações e da rede elétrica, com consequências prolongadas no tempo e de grandes proporções, apenas terminável com uma ação ofensiva com recurso a meios militares e recorrendo à força, esta justificar-se-ia, se por exemplo, estivessem em risco a vida de portugueses. Por outro lado, se no âmbito de uma operação militar, as nossas forças fossem alvo de um ciberataque, só mitigável pela destruição física das instalações inimigas a partir do qual está a ser perpetrado, então a utilização do vetor militar contra uma ação maliciosa no ciberespaço, provavelmente despoletaria uma reação cinética por um dos vetores tradicionais: mar, terra ou ar, como se de um qualquer alvo físico se tratasse.

Para tal, torna-se premente desenvolver RoE que apoiem o MDN nas suas operações no domínio do ciberespaço, a nível nacional e das Forças Nacionais Destacadas (FND). Na tabela 1 encontra-se a comparação entre as caraterísticas chave dum ciberataque relativamente a um ataque cinético, levantando as principais diferenças entre eles.

Tabela 1 - Comparação caraterísticas Ataque Cinético com Ciberataque.

Adaptado de Owens, et al (2009, p. 80).

	Ataque Cinético	Ciberataque
Efeitos significativos	Efeitos diretos normalmente mais importantes que os indiretos	Efeitos indiretos normalmente mais importantes que os diretos
Reversibilidade dos efeitos diretos	Baixa, passa pela reconstrução física e pode ser demorado	Geralmente altamente reversível num curto período de tempo
Custos de aquisição das armas	Essencialmente na procura	Essencialmente na investigação e desenvolvimento
Disponibilidade das tecnologias base	Restrita na maioria dos casos	Altamente disseminada no geral
Requisitos de Informações para o emprego	Geralmente inferiores aos requeridos para um ciberataque	Geralmente elevados se comparados com os das armas cinéticas
Incertezas no planeamento	Geralmente inferiores às associadas com um ciberataque	Geralmente elevadas se comparadas com as das armas cinéticas

Por último, deverá ser colmatada a omissão do Conceito Estratégico de Defesa Nacional, em caraterizar as ciberameaças e definir as orientações estratégicas de ciberdefesa, na prossecução da cibersegurança nacional, identificando as ICN e as I2CN, assim como, o seu nível de ambição neste domínio.

Analisaremos de seguida, o modelo a propor para um CNC, face aos indicadores apresentados anteriormente, e que integra os principais atores que a nível governamental, militar e privado desenvolvem esforços no âmbito da cibersegurança e da ciberdefesa, procurando percecionar as possíveis sinergias a obter, com uma estrutura inclusiva, promotora do diálogo e geradora de uma estratégia conjunta e holística.

b. Organização

No que concerne à vertente organizacional, os principais ensinamentos a retirar dos exemplos norte-americano e holandês, dizem respeito à necessidade de uma aposta conjunta, sinérgica e abrangente, por parte das FFAA, bem como, às vantagens decorrentes da existência de uma estrutura de coordenação interagencial e interministerial.

(1) EUA e Holanda

Os EUA através do seu CYBERCOM utilizaram os recursos do ciberespaço já existentes, de forma a criar novas sinergias e sincronizar os efeitos de combate necessários para proteger o seu ambiente de segurança da informação. Este depende do Comando Estratégico dos EUA e inclui os comandos do ciberespaço da sua Marinha, Exército e Força Aérea (DoD, 2010).

Seguindo a abordagem efetuada pela Holanda e subjacente ao seu *Dutch National Cyber Security Center*, o CNC proposto por este trabalho refletirá a parceria entre o setor público e o privado defendido ao longo da investigação, e englobará os diversos ministérios, serviços de informações, centros de investigação, empresas que constituem as ICN, assim como, os institutos académicos. No sentido de evitar a duplicação de funções, o CERT holandês fundiu-se com este centro, podendo o mesmo efetuar-se no nosso país, evitando desta forma a duplicação de infraestruturas (GOVCERT, 2012).

(2) Portugal

No sentido de se tornar também possível a nível nacional criar as sinergias necessárias no âmbito da ciberdefesa, parece de todo pertinente que o EMGFA seja o órgão diretor e coordenador a nível das FFAA, de todas as atividades a desenvolver neste domínio, usando para tal das estruturas já existentes, como o Comando Operacional Conjunto e a DICSI.

Os militares têm redes com necessidades especificas, que poderão no futuro integrar (ou não) um "Cibercentro", tornando-se necessário melhorar a organização interna ao nível da Defesa Nacional e desenvolver uma estrutura conjunta para a cibersegurança. O EMGFA, constitui o melhor órgão para atingir este desiderato, apesar de algumas limitações na sua estrutura e modo de funcionamento. A criação de raíz de uma nova estrutura poderia ficar imune aos problemas que o EMGFA padece como estrutura. (Neves, 2012)

Já identificado ao longo deste trabalho está a necessidade de criar uma entidade que coordene o esforço de cibersegurança e ciberdefesa nacionais. Foi igualmente verificado que o desenvolvimento de uma estratégia nacional de ciberdefesa terá que conjugar a componente privada com a pública. Assim, a criação de um CNC iria ter na sua vertente de Defesa, o EMGFA a coordenar as atividades a desenvolver pelas FFAA em conjugação com as valências governamentais e privadas consideradas pertinentes.

Apesar da sua dependência do MDN, o EMGFA deveria ter assento separado deste ministério no CNC, permitindo desta forma, corporizar a vertente militar da defesa nacional na alçada do CEMGFA, cabendo ao MDN a remanescente vertente não militar da ciberdefesa (Aires, 2012).

Apresenta-se na figura 1 a estrutura proposta pelo autor para o CNC português, baseado nos indicadores apresentados neste trabalho.

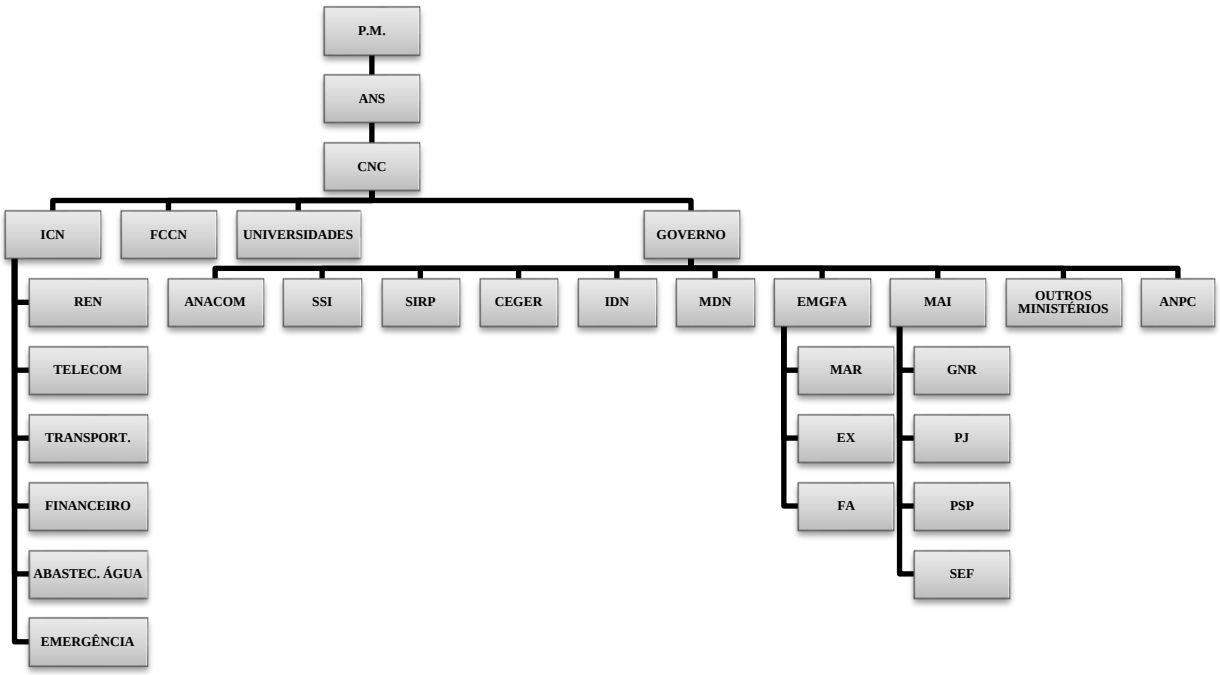

Figura 2 - Proposta de composição do Centro Nacional de Cibersegurança.

Esta estrutura engloba as principais estruturas públicas e privadas que desempenham funções no âmbito da cibersegurança, nas suas diversas vertentes, tais como, investigação e desenvolvimento, proteção das ICN, segurança e proteção da informação, assim como, na sua vertente militar, paramilitar, policial e de informações, de desenvolvimento de ações, no âmbito da segurança da informação em operações militares, na luta contra o cibercrime e na proteção da informação crítica, para a segurança do nosso país, enquanto estado democrático e integrado na comunidade internacional. Esta estrutura

com cariz de coordenação entre os atores elencados, deverá estabelecer um calendário de reuniões periódicas, bem como definir os eventos que sejam suscetíveis de desencadear a convocação do CNC.

Desde logo, na definição dos requisitos para uma doutrina nacional de cibersegurança, o CNC deveria articular-se em grupos de trabalho para escalpelizar a atual estrutura nacional e procurar identificar os organismos a eliminar, reorganizar e criar, usando os princípios da eficiência e da minimização de custos associado - como preconizado pelo GPTIC nas Resoluções do Conselho de Ministros n.º 46/2011 e n.º 12/2012 - em vez de tomar estes últimos critérios como basilares.

Mais recentemente, a resolução de Conselho de Ministros n.º 42/2012, prevê a constituíção da Comissão Instaladora do CNC, colocando-a na dependência do Primeiro-Ministro (PCM, 2012).

No que diz respeito a novas capacidades, a eficácia das mesmas passa fundamentalmente por uma capacidade de resposta integrada e coordenada, ou seja, por uma capacidade que diga respeito aos outros Ramos e ao EMGFA. As ameaças podem surgir de um ponto mais ou menos definido ou serem globais, sendo que a única forma concreta e efetiva de sucesso passa, obrigatoriamente, por ações concertadas de todos os gestores/utilizadores da rede. A recente resolução do Conselho de Ministros de criação de um CNC é sem dúvida um passo na direção certa, pelo menos no que respeita às redes do governo (Neves, 2012).

Ao nível do EMGFA, torna-se necessário reforçar a estrutura da DICSI, centralizando processos e competências, que conduzam ao aumento da massa crítica nesta divisão, composta por elementos dos três Ramos das FFAA, mas simultaneamente respeitando os seus nichos de competência e especificidades próprias (Aires, 2012).

O CNC deverá ser, adicionalmente, o fórum de discussão sobre necessidades de treino e de material, assim como, fornecer apoio na identificação de nova legislação que permita fazer face ao cibercrime e ao ciberterrorismo, em coordenação permanente com a UE e os demais países com os quais Portugal estabelece relações diplomáticas, em especial a Comunidade de Países de Língua Portuguesa (CPLP).

Para que o caminho a seguir se consubstancie e seja sustentável no tempo, torna-se necessário que haja um maior investimento na formação e treino de todos os envolvidos, e que este seja transversal a todos os atores nacionais. Vejamos de seguida, como se poderá atingir este objetivo.

c. Treino

Os requisitos de formação e treino previstos pelo EMGFA, relativamente ao pessoal envolvido na estrutura e organização da CRISI e nas atividades relacionadas com o tratamento e resposta a incidentes, uso de ferramentas e análise de vulnerabilidades, assim como, os niveis de certificação OTAN e da UE, necessários para o desempenho de funções neste domínio, vêm previstos no PEMGFA/CSI/301, bem como, o estabelecimento de relações de cooperação com entidades nacionais e internacionais, e em particular com a OTAN (EMGFA, 2008).

No que diz respeito ao treino conjunto no domínio do ciberespaço, de destacar o exercício de ciberdefesa denominado Cyber Coalition no qual Portugal participou na edição de 2010, e mais recentemente, entre 13 e 15 de dezembro de 2011, envolvendo um total de 23 nações pertencentes a esta organização, assim como seis dos seus parceiros, com o objetivo de testar as capacidade técnicas e operacionais da Aliança, face a um ataque em larga escala. O exercício foi baseado numa crise fictícia, em que todas as nações participantes tiveram de lidar com ciberataques simulados. O cenário do exercício requeria a acção, coordenação e colaboração de especialistas de ciberdefesa e órgãos de gestão.

O Secretário Geral Adjunto para os Desafios Emergentes de Segurança, o embaixador Gabor Iklody, referiu que "O número de jogadores e observadores crescente, ano após ano, demonstra a grande importância que os Aliados e seus parceiros dão à procura de uma melhor protecção contra as ciberameaças - que aumentam rapidamente - confirmando também, o reconhecimento da OTAN, como um jogador chave na ciberdefesa". O exercício permitiu adicionalmente, identificar a necessidade de colaboração da OTAN com os países parceiros. A UE participou neste exercício como observador (NATO, 2011).

No entanto, estes requisitos, assim como, a sua própria definição terão, na perspetiva do autor, que ter em consideração a hipótese previamente validada neste trabalho de que: “As capacidades de ciberdefesa nacionais terão que ser desenvolvidas de forma conjunta, combinada e integrada com as estruturas civis.”, ou seja, deverão na sua conceção ser delineados os requisitos de treino, tendo em conta o objetivo da ciberdefesa e cibersegurança nacional como um todo e não tomando as suas partes, procurando hermeticamente desenvolvê-las, esperando no final, que a sua conjugação origine as mesmas sinergias e capacidades que o crescimento conjunto trariam.

Exemplos concretos deste desiderato podem ser encontrados nas estratégias de ciberdefesa de países como a Estónia, onde é claramente identificada a necessidade de desenvolver requisitos de treino de elevada qualidade, que permitam a aquisição de competências, quer pelos agentes públicos, quer pelos agentes privados, através do estabelecimento de requisitos comuns. Por outro lado, a vertente da pesquisa e desenvolvimento nesta área deverá passar pela promoção da cooperação internacional e pelo próprio apoio na estruturação de treino de excelência. Estes requisitos assegurarão, segundo aquele país, uma maior prontidão na gestão de crises de cibersegurança, no domínio público e no privado, ao mesmo tempo que promoverá uma maior especialização e inovação no desenvolvimento e pesquisa na área da cibersegurança (Tikk, 2011a, p. 56).

O paradigma da Estónia, que como abordado anteriormente, sofreu um severo ataque às suas infraestruturas críticas nacionais em 2007, reside na forma como nação - veículado pelo CCDCoE da OTAN - tem sido pioneira no desenvolvimento da cibersegurança, não só na componente técnica, mas também no domínio concetual. Aquando dos incidentes de 2007, uma das maiores lacunas identificadas, nos organismos pertencentes às ICN daquele país, foi a falta de mão de obra qualificada na área da segurança da informação. A Estónia não possuía então, quaisquer universidades públicas ou privadas que ministrassem cursos de Bacherelato, Mestrado ou Doutoramento nesta área.

Nos últimos anos, no entanto, tem-se verificado um considerável aumento da especialização, em especial no seio do sistema financeiro, que se tem tornado num dos maiores clientes dos serviços de proteção e segurança da informação. No que toca à cibersegurança, o desenvolvimento e a pesquisa não podem ser dissociados das atividades relacionadas com a defesa (Tikk, 2011a, p. 62).

Este dualismo deverá também ser considerado na estruturação da nossa própria estratégia nacional de ciberseguraça, devendo estar patente na doutrina, organização e treino do setores público e privado.

Mas não só a Estónia reconhece a necessidade de desenvolver treino conjunto com o setor público e privado. Também a República Checa estabeleceu na sua estratégia nacional de cibersegurança, a intenção de cooperar metodicamente com o setor privado, na implementação de programas de treino que foquem a cibersegurança (Tikk, 2011a).

Na Holanda, o fortalecimento do treino e da educação, a todos os níveis, é essencial para garantir a capacidade de resistência às ameaças e para continuar a utilizar as TIC de

forma confiável. Este torna-se num pré-requisito para a expansão da economia digital (NCSS, 2011, p. 15).

Ao nível nacional, a tónica deve estar na formação técnica e profissional, nos domínios da ciberdefesa e da cibersegurança, com vista à obtenção de competências ajustadas às necessidades, e que permita a otmização efetiva destas capacidades, distanciando-se neste sentido, da uma vertente mais conceptual e académica. (Aires, 2012)

Um dos pontos indissociáveis ao meio castrense é a rotatividade dos cargos e missões que os Ramos praticam ao longo tempo, fazendo com que seja desperdiçada a longa formação e tempo necessário para atingir um grau de experiência satisfatória dos técnicos. Estes deverão possuir bons conhecimentos nas áreas das comunicações, sistemas, segurança e também da análise forense, tornando-se necessária a existência de fortes relações de confiança, entre os vários intervenientes no processo, para que a cibersegurança possa funcionar de forma efetiva (Neves, 2012).

Assim, deverão também ser analisadas as carreiras dos militares que desempenham funções neste domínio, por forma a permitir um maior aproveitamento do seu k*now-how* acumulado, sem que isso implique uma degradação das suas expetativas de progressão. Quanto maior for o grau de sofisticação dos equipamentos e tecnologias usados, menor deverá ser a rotatividade dos seus operadores, no sentido de permitir um maior aproveitamento da suas capacidades, conhecimentos e competências acumulados, assim como, permitir o aumento da massa crítica neste domínio no nosso país e em particular nas FFAA (Aires, 2012).

Analisaremos no próximo ponto, as necessidades concetuais das I2CN, para assegurar uma eficaz ciberdefesa e cibersegurança, do nosso país e das organizações internacionais em que se encontra inserido.

d. Infraestutura

As tecnologias da informação estão sujeitas a ciclos de inovação curtos. Isto significa que os aspetos técnicos e sociais do ciberespaço estão em constante mudança, criando novas oportunidades, mas também novos riscos. Pelo que, qualquer estratégia de cibersegurança deverá estar permanentemente a adaptar-se às mudanças, de forma a continuar a ser efetiva neste domínio. Se um país pretende estar preparado para responder a um ciberataque, então, torna-se necessário que seja capaz de coordenar um conjunto diversificado e abrangente de ferramentas, que lhe permita avaliar o nível de ameaça

continuamente e desenvolver em tempo útil, medidas de proteção. Os países devem avaliar se os poderes que possuem são suficientes ou se novos terão que ser atribuídos, para fazer face a estas ameaças. Este processo terá que decorrer em estreita coordenação com os setores público e privado (FMI, 2011, pp. 12 - 13).

A convergência das telecomunicações tradicionais com a internet, patente na crescente utilização desta última como meio de interligação, traz novos desafios à cibersegurança. De acordo com a Resolução do Conselho de Ministros n.º 120/2008, de 30 de julho, as comunicações eletrónicas estão a evoluir para um modelo de redes convergentes de multisserviços, baseadas em tecnologias integradoras, que possuem novas potencialidades e a capacidade de integrar serviços de voz, internet, televisão, entre outras. A evolução deste tipo de redes culminou com o recente lançamento das redes 4G/*Long Term Evolution*, que não só permitirá um aumento das velocidades de transferência de dados através da rede, mas também trará uma arquitetura totalmente baseada em *Internet Protocol* (IP), beneficiando de uma maior integração e convergência com as redes fixas (Alveirinho, 2011).

Nas redes *Legacy*[16], a utilização da internet estava dissociada das telecomunicações e não permitia a transferência dos grandes volumes de informação, que as redes atuais permitem hoje em dia, em que praticamente tudo que esteja relacionado com ligações de vídeo, voz e dados passa por um protocolo TCP[17]/IP. Um ciberataque tem desta forma um efeito disruptivo potencialmente maior, e os seus efeitos, a capacidade para fazer viajar no tempo uma sociedade moderna da era do conhecimento, para outra da revolução industrial do século XIX.

A par da evolução tecnológica das próprias redes, também os equipamentos de segurança e proteção terão que evoluir. Esta evolução terá forçosamente que ser continua e acarretará custos avultados. A tabela 2 sistematiza as vulnerabilidades, ameaças e ataques que se podem considerar, relativos a um centro de dados, e sobre as quais as capacidades de ciberdefesa deverão incidir.

[16] Termo usado para definir uma rede baseada em protocolos antigos e obsoletos que não têm por base o protocolo IP (TCP/IP). No caso das redes sem fios, refere-se às redes que têm por base o protocolo 802.11x. (Webopedia, 2012)
[17] TCP – *Transmition Control Protocol* (Webopedia, 2012).

Tabela 2 - Categorias de vulnerabilidades, ameaças e ataques.

Adaptado de Saadawi et al (2011, p. 201).

Vulnerabilidades	Ameaças	Ataques
Conceção	Intrusão	*DoS e DDoS*
Tecnologias	*Spam*	Acesso não autorizado
Aplicações	*Worm*	Adulteração de informação
Base de dados	Vírus	*Cross-site scripting*
Redes	*Malware*	IP *spoofing*
Ferramentas de monitorização	*Spyware*	Atividades maliciosas a partir do interior

Do ponto de vista da proteção das infraestruturas críticas da informação, as principais atividades que deverão ser desenvolvidas, para garantir uma melhoria na efetividade da ciberdefesa nacional, passarão por uma análise dos constituintes do CNC proposto e culminarão na redefinição de requisitos, por um grupo de trabalho composto por especialistas a nomear pelo CNC. Neste sentido, indicar-se-ão de seguida, algumas propostas que permitirão, de acordo com o CCDCoE, indicar um possível caminho a seguir.

Assim, inicialmente deverão ser identificados e elencados os serviços e componentes das I2CN, entendidos aqui como aqueles que são imprescindíveis para garantir o funcionamento das mesmas. Deverá depois, determinar-se quais as interdependências existentes nas I2CN, o que permitirá o desenvolvimento de uma metodologia de análise das suas vulnerabilidades e dos respetivos serviços de apoio. Finalmente, deverá efetuar-se uma análise de risco à cibersegurança, onde se recolherão informações sobre a situação atual no ciberespaço, de forma a planear ações preventivas e identificar as contramedidas necessárias, para lidar com ataques à cibersegurança nacional. O processo contínuo de assegurar este objetivo último, passará por avaliações de risco periódicas (Tikk, 2011a, p. 70).

A 14 de Abril de 2011, a DICSI considerou que o essencial da componente de *backbone* da rede de comunicações das FFAA, integra a Rede Fixa de Transporte e Roteamento (RFTR). O *backbone* é materializado por várias componentes e a sua

identificação física, RFTR, redes satélite e outras redes (i.e. HF, VHF, UHF, Wi-Fi), será progressiva. A RFTR consiste numa malha de troços interligados por nós, materializada em tecnologias diversas (atualmente Fibra Ótica) e feixes hertzianos por onde circulam dados e informação, com graus de importância variável e que cobre o território nacional. O encaminhamento dos dados entre utilizadores deverá evoluir da atual geometria comutada (circuitos ponto a ponto), para a modalidade de roteamento caracterizado por um percurso com geometria variável, em função da disponibilidade instantânea de recursos dos troços e nós e da prioridade atribuída (Aires, 2012).

Pretende-se a edificação duma Rede Fixa Nacional para o transporte e roteamento de alto débito e de processamento automático de informação, entre os órgãos de comando e controlo, para que qualquer um destes órgãos tenha capacidade, em tempo real, para recolher, relacionar, processar, aceder e difundir informação, tendo em vista o apoio à tomada de decisão, ao nível do CEMGFA e dos Chefes de Estado-Maior dos Ramos, sobre o empenhamento do dispositivo de forças, tendo em mente a sua prontidão, disponibilidade, sustentação e emprego das forças e meios (Aires, 2012).

Em termos estratégicos é desejável que a RFTR seja em fibra ótica e com capacidade instalada, para permitir atribuição dos recursos de transporte e comunicação, em função da procura instantânea, da prioridade estabelecida pelos requisitos operacionais do exercício de comando e controlo, e tipo de informação *Quality of Service* (Aires, 2012).

Em função da arquitetura da rede e do encargo operacional das entidades utilizadoras, há que definir que troços da RFTR devem estar ligados por fibra ótica - detida pelas FFAA - assim como, os que podem e até quando, permanecer em feixes hertzianos e aqueles para os quais se reconhece vantagem em que funcionem com recurso à contratação externa (transporte, ou só aluguer de meio de transporte). Trata-se de uma infraestrutura de uso partilhado, construída a partir da década de 80 do século passado, e predominantemente sob a alçada do EMGFA. Administrá-los como um todo, potencia a eficiência na gestão do ciclo de vida das tecnologias utilizadas. Importa promover a atualização da atual infraestrutura, promovendo a eficiência e a eficácia, o que sugere que a sua administração seja efetuada por uma única entidade. A sua implantação inicial e o atual enquadramento legislativo sugerem que a entidade administrante seja o EMGFA/DICSI (Aires, 2012).

Tendo a infraestrutura as características acima referidas, na opinião do autor, seria possível, garantir a necessária resiliência, sem a qual de nada servirão, por melhores que sejam, os contributos da doutrina, organização e treino para a cibersegurança nacional.

Analisamos neste capítulo as principais linhas de atuação, necessárias para fomentar a cibersegurança, e assim permitir uma melhoraria na capacidade de ciberdefesa e da forma como esta deverá ser desenvolvida. Desde logo estabelecendo o ponto de situação a nível nacional do GPTIC, focando no embrião do futuro CNC e da ENSI. Formulando-se de seguida, as questões basilares sobre o processo de criação de uma doutrina nacional, que seja integradora do setor público e privado, e que mantenha uma estreita ligação com a comunidade internacional. Propôs-se uma estrutura para o CNC com base neste desiderato, apresentando a ANS com o órgão coordenador a nível nacional para a cibersegurança. Abordou-se finalmente os indicadores relativos ao treino e infraestruturas nacionais.

Partindo das duas hipóteses previamente validadas e dos indicadores elencados ao longo do trabalho, associando os apresentados neste último capítulo, foi possível responder à pergunta de partida desta investigação: *"De que forma será necessário desenvolver as atuais capacidades de ciberdefesa nacionais, de forma a permitir uma eficaz cibersegurança relativamente às vulnerabilidades críticas da infraestrutura da informação?"*.

Assim, as atuais capacidades de ciberdefesa nacionais deverão ser desenvolvidas de forma coordenada entre as todas as entidades nacionais interessadas, englobando o setor público, onde se inserem o Governo, as FFAA, as Forças de Segurança, a Proteção Civil e os Serviços de Informações - o setor privado, as instituições académicas, e as ICN, tais como, a Rede Elétrica Nacional, as Telecomunicações, os Transportes, a Rede de Distribuição de Água ou os Serviços de Emergência. As sinergias a criar permitirão, que logo na sua génese, se construa uma nova e holística ENSI, onde exista o diálogo permanente entre todos os atores nacionais e internacionais, no sentido de permanentemente efetuar uma avaliação dos riscos associados com as ciberameaças, e desta forma, adaptar-se e permitir uma continua melhoria da resiliência e segurança das I2CN, por consequência das ICN e por fim de Portugal, como nação democrática que procura a integração internacional e não a redutora infoexclusão.

Conclusões

Em Portugal não está definida ainda uma estratégia de cibersegurança, não existindo entidades primariamente responsáveis e formalmente mandatadas, do ponto de vista legal, para exercer a coordenação de uma resposta concertada ao nível político, estratégico, ou militar. Diversas entidades civis como a FCCN ou o CERT atuam sob o ponto de vista de coordenação de respostas nacionais no âmbito da cibersegurança, ainda que não possuindo um mandato do Governo para tal. Urge a definição de uma política de cibersegurança e de uma estratégia para a sua implementação. Sendo esta uma área de soberania, o Estado não a deverá delegar.

Pretendeu-se com presente trabalho, estabelecer um ponto de situação a nível nacional, sobre as capacidades de ciberdefesa, e identificar quais as medidas a desenvolver nas novas capacidades neste domínio, considerando os elementos ou componentes respetivos (doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade), no âmbito da Defesa Nacional e das FFAA. Para tal formulou-se a seguinte pergunta de partida:

> *"De que forma será necessário desenvolver as atuais capacidades de ciberdefesa nacionais, de forma a permitir uma eficaz cibersegurança relativamente às vulnerabilidades críticas da infraestrutura da informação?"*.

A pergunta de partida levou a duas perguntas derivadas:

PD1. *"Em que medida a atual capacidade de ciberdefesa nacional será eficaz para fazer face a um ciberataque?";*

PD2. *"De que forma será necessário desenvolver as capacidades de ciberdefesa nacionais para melhorar e complementar as existentes?".*

Diversas são as entidades que a nível público e privado desenvolvem esforços para melhorar a capacidade de ciberdefesa e a cibersegurança nacionais, tendo sido identificadas diversas lacunas a resolver.

Sendo a Segurança e Defesa funções essenciais do Estado, deverá ser o Estado - agente primordial na garantia do objetivo teleológico de segurança - a liderar e promover uma ENC, integrando-a na sua própria estratégia de *e-Government* e conduzindo-a como uma das suas ações executivas, num momento onde a proteção das I2CN, se tornou não só numa necessidade como um imperativo, de que os repetidos ataques de piratas informáticos ligados a um grupo intitulado LulzSec Portugal se tornam exemplo.

A necessidade de um CNC foi já identificada por várias entidades, subsistindo a dúvida se deve ser criada uma nova estrutura ou aproveitadas as já existentes, congregando os três Conselhos Superiores de Defesa, Administração Interna e de Informações. Tendências recentes apontam para a criação deste órgão coordenador na ANS.

Também a nível militar o ciberespaço se constitui como uma nova dimensão que requer ponderação. As guerras no ciberespaço trazem graves consequências, apesar dos reduzidos custos envolvidos, sendo dificilmente identificados os seus autores. A consciencialização por partes das Nações de que existe hoje em dia um novo vetor da guerra – a ciberguerra – que coexiste com os tradicionais mar, terra, ar e espaço, deverá originar a aquisição de novas capacidades, que lhe permita criar forças nesta vertente. Os atores que não desenvolvam esforços neste domínio, serão suplantados pelos seus adversários, ficando em desvantagem face ao atual ambiente caracterizado por uma forte competição.

O EMGFA, através da sua publicação PEMGFA / CSI / 301, prevê já a implementação da CRISI-FA, como forma de responder de forma concertada a incidentes de segurança informática, relacionados com atividades de *software* malicioso, atividades de utilizadores não autorizados, negação de serviços, ou outras ameaças e vulnerabilidades inerentes às CSI, utilizando de forma coordenada as valências existentes nos Ramos das FFAA e no EMGFA, disponibilizando serviços reativos, pró-ativos e de gestão de segurança e qualidade de serviço.

Por outro lado, a DICSI do EMGFA desempenha a missão de apoio às áreas de planeamento, direção e controlo dos sistemas de informação e tecnologias de informação e comunicação, inerentes ao comando e controlo nas FFAA, sendo sua responsabilidade promover a implementação da política conjunta de segurança da informação, de forma a garantir a autonomia, sobrevivência e interoperabilidade dos sistemas das FFAA. No entanto, são várias ainda as vulnerabilidades detetadas nas FFAA. A criação de uma estrutura nova, de raiz, poderia ficar imune aos problemas que o EMGFA padece como estrutura.

No sentido de estabelecer áreas de competência para os diferentes atores nacionais, que no âmbito da cibersegurança enfrentam os problemas de segurança específicos do ciberespaço - as forças de segurança ficariam responsáveis pelas áreas do cibercrime e do ciberativismo; e o SIS pelas relativas ao ciberterrorismo e à ciberespionagem. No contexto do ciberespaço, às FFAA seria atribuída incumbência da ciberdefesa. Todas estas entidades

desenvolveriam na sua esfera de atuação, esforços para prevenir, detetar, defender e recuperar face a ciberataques.

A CRP fornece as bases legais que permitem consubstanciar este modelo. No entanto, ao nível dos Ramos das FFAA, as capacidades de ciberdefesa cingem-se quase exclusivamente à sua própria proteção, não existindo uma doutrina comum de emprego conjunto para criar sinergias adicionais a nível da defesa nacional.

O setor privado possui a infraestrutura do ciberespaço, pelo que se torna essencial no desenvolvimento de uma estratégia de cibersegurança nacional, assumindo-se como um ator importante no desenvolvimento das capacidades de ciberdefesa, as instituições académicas. Neste contexto, torna-se importante estabelecer parcerias público-privadas, efetuando a sua integração com as estruturas militares, na criação de uma estratégica eficaz de cibersegurança. Por outro lado, a própria doutrina nacional deverá ser desenvolvida em conjugação com entidades públicas e privadas.

Uma estratégia de cibersegurança deverá estar assente em dois pilares sólidos: um robusto relacionamento internacional e o livre fluxo de informação, ao que se associam os princípios de abertura, interoperabilidade, segurança e fiabilidade. Assim, a cooperação entre as nações aliadas deverá compreender a partilha das capacidades de aviso prévio e de boas práticas identificadas, num esforço de desenvolvimento de capacidades e de treino conjuntos. Um dos desafios ao desenvolvimento da cibersegurança preconizado, são as diferenças culturais que terão que ser vencidas, no sentido de permitir a harmonização da parceria entre Estado, FFAA e setor privado.

As ICN dependem estruturalmente da eletricidade e funcionalmente dos sistemas de informação, a rede de distribuição de energia elétrica depende também funcionalmente dos sistemas de informação, pelo que desta constatação poderemos concluir quanto à importância para o país, da necessidade de garantir a segurança dos sistemas de informação. Neste domínio, o centro de gravidade do risco social, está nas redes de telecomunicações.

Os indicadores recolhidos claramente apontam para existência de um esforço nacional a nível da ciberdefesa e da cibersegurança, englobando os setores governamental, civil e militar. No entanto, evidencia pouca articulação e coordenação destes atores essênciais da sociedade de informação, e até mesmo dos Ramos das FFAA, os quais apresentam ainda diversas vulnerabilidades e dificuldades de integração concetual e operacional. A falta de uma estratégia nacional de ciberdefesa, contendo uma entidade

coordenadora e mandatada para harmonizar e gerar as sinergias necessárias, para alcançar o desiderato da efetiva capacidade de prevenção, deteção, defesa e recuperação contra um ciberataque, que permita a proteção das ICN, contribui para as deficiências apontadas neste trabalho. Assim, foi possível responder à primeira pergunta derivada *"Em que medida a atual capacidade de ciberdefesa nacional será eficaz para fazer face a um ciberataque?"* ao validar a primeira hipótese formulada *"A atual capacidade de ciberdefesa nacional é ineficaz para fazer face a um ciberataque."*.

Efetuou-se de seguida uma análise às capacidades internacionais no âmbito da ciberdefesa, criando o enquadramento basilar para a sua conceptualização, procurando desta forma, percecionar o estado da arte a nível internacional e recolher indicadores que permitam concluir quanto a uma estratégia nacional de ciberdefesa.

A perceção global sobre as ciberameaças mudou drasticamente depois dos ciberataques ao governo da Estónia em 2007. Antes do incidente naquele país, as organizações tendiam a tratar isoladamente os riscos com que lidavam.

Também no plano legal houve necessidade de adaptação às novas ameaças, uma vez que estas põem à prova os limites da legislação existente sobre proteção da informação, comunicações eletrónicas e de acesso às informações públicas. Desde 2007, a OTAN, a ONU, e a UE, entre outras organizações internacionais, introduziram novas políticas de cibersegurança ou reviram as antigas.

Patente nos indicadores recolhidos e apresentados, está não só o esforço dedicado pela comunidade internacional, mas também a necessidade identificada de coordenar e estimular a cooperação interna entre o setor privado e público, assim como, no plano externo, a criação de parcerias multinacionais que fomentem o desenvolvimento de capacidades de ciberdefesa, como são exemplo a UE, os EUA ou a OTAN, através do seu CCDCoE.

Desta forma, foi possível responder à segunda pergunta derivada "*De que forma será necessário desenvolver as capacidades de ciberdefesa nacionais para melhorar e complementar as existentes?*" ao validar a segunda hipótese formulada "*As capacidades de ciberdefesa nacionais terão de ser desenvolvidas de forma conjunta, combinada e integrada com as estruturas civis.*".

Na continuação da última parte da investigação, foram abordadas as estratégias implementadas internacionalmente e que se consideram de relevo, procurando transpô-las

para o plano nacional, elencando os requisitos necessários para o desenvolvimento das capacidades de ciberdefesa e cibersegurança.

A doutrina, a organização e o treino, devem ser desenvolvidos na sua génese, integrando o Estado, as FFAA e o setor privado, e procurando estabelecer ligações com a comunidade internacional, de forma a assegurar a eficaz proteção e defesa das ICN e das I2CN, contribuindo dessa forma para a cibersegurança nacional. No entanto, estas três vertentes da definição de novas capacidades neste domínio, dependem de uma infraestrutura resiliente e robusta para fazer face a ciberataques. O encaminhamento dos dados entre utilizadores deverá evoluir da atual geometria comutada, para uma com geometria variável. Pretende-se a edificação duma Rede Fixa Nacional para o transporte e roteamento de alto débito e de processamento automático de informação, entre os órgãos de comando e controlo, ao nível do CEMGFA e dos Chefes de Estado-Maior dos Ramos, sobre o empenhamento do dispositivo de forças.

A RFTR deverá ser administrada como um todo, potenciando a eficiência na gestão do ciclo de vida das tecnologias utilizadas. A sua implantação inicial e o atual enquadramento legislativo sugerem que a entidade administrante seja o EMGFA/DICSI, indo de encontro à necessidade previamente identificada, de uma maior centralização num órgão coordenador ao nível das FFAA.

As duas hipóteses previamente validadas e os indicadores elencados ao longo do trabalho, tornaram possível responder à pergunta de partida desta investigação: *"De que forma será necessário desenvolver as atuais capacidades de ciberdefesa nacionais, de forma a permitir uma eficaz cibersegurança relativamente às vulnerabilidades críticas da infraestrutura da informação?"*. Assim, foi possível concluir que as atuais capacidades de ciberdefesa nacionais deverão ser desenvolvidas de forma coordenada entre todas as entidades nacionais interessadas, englobando o setor público, privado, as instituições académicas, e as ICN.

As sinergias a criar permitirão, que logo na sua génese, se construa uma nova e holística ENSI, onde exista o diálogo permanente entre todos os atores nacionais e internacionais, no sentido de permanentemente efetuar uma avaliação de risco, associado com as ciberameaças e dessa forma, adaptar-se e permitir uma continua melhoria da resiliência e segurança das I2CN, por consequência das ICN e por fim de Portugal, como nação democrática, que procura a integração internacional e não a redutora infoexclusão.

Recomendações

Face ao exposto, e porque no âmbito da Defesa Nacional, se concluiu ser crucial centralizar o papel de coordenação, no seio das Forças Armadas, tecem-se as seguintes recomendações ao seu Estado-Maior General:

- Promover a criação de um Grupo de Trabalho para a Ciberdefesa Nacional, composto por representantes das áreas das TIC dos três Ramos, de forma a permitir o debate periódico da situação atual das ciberameaças, e estabelecer o ponto de situação face às capacidades existentes para as enfrentar e que possa integrar o Centro Nacional de Cibersegurança, contribuindo para o esforço de cibersegurança nacional;

- Centralizar na DICSI, um órgão coordenador de ciberdefesa, que coordene de forma centralizada, as já existentes estruturas dos Ramos neste domínio, de forma a possibilitar o desenvolvimento de capacidades conjuntas, fomentando a ligação e a partilha de informação;

- Criar doutrina conjunta de ciberdefesa, em coordenação com os parceiros internacionais e com as estruturas governamentais e privadas, propondo a definição das RoE nacionais para a atuação das FFAA;

- Rever e atualizar o PEMGFA/CSI/301, fomentando a visão e a operação em conjunto;

- Desenvolver esforços para efetuar o tratamento de dados e a correlação de eventos, ao nível do EMGFA e dos Ramos, de forma a aumentar o conhecimento sobre as ciberameaças a fim de desenvolver métodos para minimizar as vulnerabilidades da nossa I2CN;

- Reavaliar os requisitos de treino e formação dos militares, no sentido de promover e fomentar a participação em fóruns nacionais e internacionais de debate e divulgação de matérias relacionadas com a ciberdefesa e cibersegurança;

- Reequacionar os períodos de rotatividade para os militares da área das TIC, de forma a garantir um maior aproveitamento da sua formação e *know-how* acumulados.

Bibliografia

Aires, M. J. M. C. (MGen/ENGEL), 2012. Entrevista com o Chefe da *DICSI/EMGFA.* Entrevistado por Cap/PILAV Nuno Monteiro da Silva. Lisboa. [Entrevista] (11 Abr. 2012).

Alveirinho, L., 2011. *Jornal Fibra.* [Em linha]
Disponível em: www.fibra.pt/opiniao/1522-a-geracao-que-esta-a-porta.html
[Consult. 02 Abr. 2012].

Alves, P. C., 2012. *Capacidades de Ciberdefesa da Força Aérea.* Entrevistado por Cap/PILAV Nuno Monteiro da Silva. Lisboa. [Entrevista] (27 02 2012).

Amaro, J. B., 2011. *Jornal Público.* [Em linha]
Disponível em: http://publico.pt/Tecnologia/nova-vaga-de-ataques-informaticos-aos-sites-do-parlamento-psp-e-financas-1523184?all=1
[Consult. 23 Jan. 2012].

ANACOM, 2012. *Autoridade Nacional de Comunicações.* [Em linha]
Disponível em: http://www.anacom.pt/render.jsp?contentId=1072476
[Consult. 18 Jan. 2012].

Anil, S., 2011. *Organização do Tratado do Atlântico Norte.* [Em linha]
Disponível em: http://www.nato.int/cps/en/natolive/news_80764.htm?selectedLocale=en
[Consult. 16 Jan. 2012].

AR, 2009. *Lei do cibercrime* (Lei n.º 109/2009, de 15 de setembro), Lisboa: Diário da República.

Brundidge, B. G. G. L., 2011. *Partnerships in Cyber Security.* Lisboa, s.n.

Caldas, A., 2011. *Uma Estratégia Nacional de Ciberdefesa (ENC).* Segurança e Defesa, janeiro - março, pp. 94 - 98.

CCDCOE, 2011. *Centro de Excelência de Ciberdefesa Cooperativa da OTAN.* [Em linha]
Disponível em: http://www.ccdcoe.org
[Consult. 22 Fev. 2012].

CEGER, 2012. *Centro de Gestão da Rede Informática do Governo.* [Em linha]
Disponível em: http://www.ceger.gov.pt/
[Consult. 16 Jan. 2012].

Conley, H. A. & Darnis, J.-P., 2011. *EU-US Security Strategies: Comparative Scenarios and Recommendations.* Bruxelas, s.n.

CRP, 2005. *Constituição da Republica Portuguesa - Sétima Revisão Constitucional* (Lei Constitucional n.º 1/2005), Lisboa: Diário da República.

CSIS, C. f. S. a. I. S., 2012. [Em linha]
Disponível em:
http://csis.org/files/publication/111220_Significant_Cyber_Incidents_Since_2006.
[Consult. 30 Jan. 2012].

DoD, 2010. *US Department of Defese.* [Em linha]
Disponível em:
http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf
[Consult. 01 Abr. 2012].

EMGFA, 2008. *PEMGFA/CSI/301.* Lisboa: EMGFA.

EMGFA, 2012. *Estado-Maior General das Forças Armadas.* [Em linha]
Disponível em: www.emgfa.pt
[Consult. 02 Abr. 2012].

ENISA, 2012. *ENISA.* [Em linha]
Disponível em: http://www.enisa.europa.eu/about-enisa
[Consult. 01 Mar. 2012].

Eurostat, 2012. *Eurostat.* [Em linha]
Disponível em: http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/
[Consult. 13 Jan. 2012].

Ewell, S. A., 2011. *Partnerships in Cyber Security.* Instituto da Defesa Nacional, s.n.

FCCN, 2012. *Computer Emergengy Response Team.* [Em linha]
Disponível em: http://www.cert.pt/index.php/pt/institucional/enquadramento-e-motivacao
[Consult. 18 Jan. 2012].

FMI, G. F. M. o. I., 2011. *Cyber Security Strategy for Germany.* 1ª ed. Berlim: Department IT 3.

Fonseca, P., 2011. *Computer World Portugal.* [Em linha]
Disponível em: http://www.computerworld.com.pt/2011/05/03/portugal-sem-estrategia-coordenada-de-ciberseguranca/
[Consult. 23 Jan. 2012].

GNS, 2012. *Gabinete Nacional de Segurança.* [Em linha]
Disponível em: http://www.gns.gov.pt
[Consult. 19 Jan. 2012].

Gouveia, J. B., 2012. *Seminário "Ciberespaço: Espaço Virtual, Mediático e Global".* Academia de Ciência de Lisboa, Disponível em http://www.jorgebacelargouveia.com/2512012-direito-do-ciber-espaco-academia-de-ciencias-de-lisboa.html.

GOVCERT, 2012. *GOVCERT.NL.* [Em linha]
Disponível em: www.govcert.nl
[Consult. 01 Abr. 2012].

JointStaff, 2006. *Joint Publication 3-13 - Information Operations.* 1 ed. EUA: s.n.

Kempf, A., 2011. *Center for Strategic and International Studies.* [Em linha]
Disponível em: http://csis.org/blog/considerations-nato-strategy-collective-cyber-defense
[Consult. 12 Mar. 2012].

Krishna-Hensel, S. F., Mauer, V. & Cavelty, M. D., 2007. *Power and Security in the Information Age: Investigating the role of the state in cyberspace.* 1 ed. Burlington: Ashgate Publishing Limited.

Leandro, T. G. et al., 2000. *A Gestão da Informação e a Tomada de decisão.* 1ª Edição ed. Sintra: Atena.

Lino, P. B., 2011. *Minutas publicadas do discurso do Secretário de Estado Adjunto e da Defesa Nacional no Seminário Internacional "Ciberespaço e Estratégia Nacional de Informação".* IDN, Lisboa, s.n.

Luís, A., 2012. *Conferência no IESM sobre o Sistema de Segurança Interna ao CEMC 2011-2012.* Entrevistado por Cap/PILAV Nuno Monteiro da Silva. Lisboa. [Entrevista] (30 Jan. 2012).

Macedo, M., 2012. *Governo de Portugal.* [Em linha]
Disponível em:
http://www.portugal.gov.pt/media/466392/20120216_mai_ciberseguranca.pdf
[Consult. 22 Mar. 2012].

Magalhães, P. D. L. T., 2012. *Seminário "Ciberespaço: Espaço Virtual, Mediático e Global".* Academia de Ciências de Lisboa, s.n.

Mascarenhas, T.-G. A. J. M. d., 2012. *Conferência da Unidade Curricular de Planeamento Estratégico do CEMC 2011/2012.* IESM, s.n.

MDN, 2011. *Estabelece os procedimentos de identificação e de protecção das infraestruturas essenciais para a saúde, a segurança e o bem estar económico e social da sociedade nos sectores da energia e transportes* (Decreto-Lei n.º 62/2011, de 9 de maio), Lisboa: Diário da Republica.

MEC, M. d. E. e. C., 2012. *UMIC - Agência para Sociedade do Conhecimento, IP.* [Em linha]
Disponível em:
http://www.umic.pt/index.php?option=com_content&task=section&id=18&Itemid=186
[Consult. 25 Jan. 2012].

Miranda, V. & Di Camillo, F., 2011. *EU - US Security Strategies: Comparative Scenarios and Recommendations (Executive Summary),* Bruxelas: s.n.

Morais, L., Silva, O., Seabra, M. & Luís, A., 2011. *Cyberwar - Definição, possibilidades de desenvolvimento de um modelo nacional de implementação.* Lisboa: IESM.

MOSTI, T. e. I. d. M., 2012. *Ministério da Ciência, Tecnologia e Inovação da Malásia - MOSTI.* [Em linha]

Disponível em: http://www.nitc.my/index.cfm?&menuid=60
[Consult. 05 Abr. 2012].

NCSS, 2011. *The National Cyber Security Strategy - Success Through Cooperation.*. Holanda: s.n.

Neves, P. B. d., 2012. *Capacidades de Ciberdefesa da Marinha.* Entrevistado por Cap/PILAV Nuno Monteiro da Silva. Lisboa. [Entrevista] (29 03 2012).

Nunes, P. F. V., 2009. *Mundos Virtuais, Riscos Reais: Fundamentos para a definição de uma Estratégia da Informação Nacional,* s.l.: CINAMIL e CIIWAC.

Nunes, P. V., 2012a. *Capacidades de Ciberdefesa do Exército.* Entrevistado por Cap/PILAV Nuno Monteiro da Silva. Lisboa. [Entrevista] (12 01 2012a).

Nunes, P. V., 2012b. Academia de Ciências de Lisboa, s.n.

OTAN, 2006. *Research and Tecnhology Organization - Technical Report: TR-071-06.* [Em linha]
Disponível em: http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-071///TR-071-06.pdf
[Consult. 22 Mar. 2012].

OTAN, 2010a. *NATO Glossary of terms and definitions - AAP-6.* Bruxelas: OTAN.

OTAN, 2010b. *Organização do Tratado do Atlântico Norte.* [Em linha]
Disponível em: http://www.nato.int/cps/en/natolive/topics_49158.htm
[Consult. 10 Nov. 2011].

OTAN, 2010c. *Strategic concept for the defense and security of the members of the North Atlantic Treaty Organization.* Lisboa: s.n.

OTAN, 2011a. *Organização do Tratado do Atlântico Norte.* [Em linha]
Disponível em: http://www.nato.int/cps/en/natolive/news_80764.htm?selectedLocale=en
[Consult. 16 Jan. 2012].

OTAN, 2011b. *Organização do Tratado do Atlântico Norte.* [Em linha]
Disponível em: http://www.nato.int/cps/en/SID-2B16B303-

7AA0A414/natolive/news_75195.htm?selectedLocale=en
[Consult. 12 Mar. 2012].

OTAN, 2011c. *Organização do Tratado do Atlântico Norte.* [Em linha]
Disponível em: http://www.nato.int/cps/en/SID-F76CE9A5-C49C79B9/natolive/news_82213.htm
[Consult. 01 Mar. 2012].

Owens, W. A., Dam, D. W. & Lin, H. S., 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberatacks Capabilities.* 1 ed. Washington : The National Academies Press.

PCM, 2012. *Aprova o plano global estratégico de racionalização e redução de custos com as Tecnologias de Informação e Comunicação na Administração Pública, apresentado pelo Grupo de Projeto para as Tecnologias de Informação e Comunicação* (Resolução do Conselho de Ministros n.º 42/2012, de 5 de abril), Lisboa: Diário da República.

Peterson, L. L. & Dawie, B. S., 2007. *Computer Networks: A Systems Approach.* 1ª ed. San Francisco: Elsevier.

QUIVY, R. C. L. V., 2005. *Manual de Investigação em Ciências Sociais.* 4 ed. Lisboa: Gradiva.

Rascão, J. P., 2008. *Novos Desafios da Gestão da Informação.* 1 ed. Lisboa: Silabo.

Saadawi, T. & Jordan, L., 2011. *Cyber Infrastructure Portection.* 1ª ed. EUA: US Army War College.

SCEE, 2012. *Serviço de Certificação Eletrónica do Estado.* [Em linha]
Disponível em: http://www.scee.gov.pt/
[Consult. 16 Jan. 2012].

Silva, C. M. P. G. M. d., 2010. *TAI - A Influência da Cibersegurança na Ordem Internacional.* Lisboa: IESM.

Sun Tzu, *The Art of War.* 2009. Traduzido do chinês por Giles, L., *Classic Edition.* El Paso, Texas: El Paso Norte Press, p. 39.

Tikk, E., 2011a. *Frameworks for International Cyber Security - National Cyber Security Policies and Strategies.* Tallin: CCD COE Publications.

Tikk, E., 2011b. *Ten Rules for Cyber Security.* 1ª ed. Tallin: CCDCOE.

UE, 2010. *UE.* [Em linha]
Disponível em:
http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm
[Consult. 30 Jan. 2012].

Watts, N., 2011. Web watching: keeping an eye on cyber threats. 26 outubro, p. 22.

Webopedia, 2012. *Webopedia.* [Em linha]
Disponível em: www.webopedia.com/term/L/legacy_network.html
[Consult. 02 Abr. 2012].

WhiteHouse, 2009. *Casa Branca.* [Em linha]
Disponível em:
www.whitehouse.gov/assets/documents/cyberspace_policy_review_final.pdf
[Consult. 01 Abr. 2012].

Zorrinho, C., 1995. *Gestão da Informação - Condição para Vencer.* s.l.:IAPMEI

APÊNDICE 1

Corpo de Conceitos.

Capacidade de Ciberdefesa Nacional - Conjunto de valências que se destinam à prevenção, deteção, defesa e recuperação de ciberataques contra a infraestrutura da informação a nível nacional.

Ciberameaça - Capacidade passível de ser utilizada para perpetrar um ciberataque.

Ciberataque - Ação deliberada ou inintencional realizada no ciberespaço e que provoque direta ou indiretamente consequências negativas no domínio governamental, militar ou civil.

Ciberdefesa - Conjunto de valências e ações que se destinam à prevenção, deteção, defesa e recuperação de ciberataques, e que contribuem dessa forma para a cibersegurança.

Cibersegurança – Estado de não existência de perigo ou possibilidade de danos causados pela disrupção das TIC ou fruto de ações abusivas destas.

***Computer Network Operations* -** Capacidade de suporte às operações militares que é empregue, juntamente com a Guerra Eletrónica, no ataque, deceção, degradação, disrupção, negação, exploração e defesa de informação eletrónica e suas infraestruturas. Divide-se em *Computer Network Attack* (CNA) e *Computer Network Defense* (CND) (JointStaff, 2006).

Dados - Elementos básicos e não processados que se constituem como componentes primários de uma determinada infraestrutura de informação.

Informação - Objeto criado pelo homem com a finalidade de representar um acontecimento identificável por ele no mundo real, integrando e relacionando um conjunto de registos ou dados (Rascão, 2008, p. 68).

***Information Assurance* -** Medidas que protegem e defendem sistemas de informação, garantindo a sua disponibilidade, integridade, autenticação, confidencialidade e não-repúdio. Incorpora capacidades de deteção e reação que permitam a proteção e recuperação dos sistemas de informação (JCS, 2006).

Information Superiority - A vantagem operacional derivada da capacidade de coletar, processar e disseminar um fluxo ininterrupto de informações, enquanto explora ou nega essa mesma capacidade no adversário (JCS, 2006).

Infraestrutura Crítica Nacional (ICN) - Componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções (MDN, 2011, p. 2624).

Infraestrutura Crítica Europeia (ICE) - Infraestrutura crítica situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um Estado-Membro da UE, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas (MDN, 2011, p. 2624).

Infraestrutura de informação Crítica Nacional (I2CN) – Conjunto de sistemas reais, virtuais e funções que são vitais para a Nação e cuja incapacitação ou destruição teria um impacto devastador sobre a economia, imagem, defesa e segurança nacional, assim como, sobre a capacidade do governo para exercer as suas funções e para a saúde e segurança pública (MOSTI, 2012).

Operações de Informação - Coordenação e sincronização do emprego de capacidades no apoio à consecução dos objetivos do comando ou para prevenir o adversário de os atingir. Compreende cinco capacidades essenciais: Operações Psicológicas (PSYOPS); Deceção Militar (MILDEC); Segurança das Operações (OPSEC); Guerra Eletrónica (EW) e CNO (JCS, 2006).

Sistema de Informação - Conjunto composto por equipamentos, métodos e procedimentos, e se necessário, pessoal, organizado para desempenhar funções de processamento de informação (OTAN, 2010, p. 2-I-4).

Tecnologias da Informação e Comunicação - Conjunto de conhecimentos, meios materiais e *know-how*, necessários à produção, comercialização e ou utilização de bens e serviços, relacionados com o armazenamento temporário ou permanente dos dados, bem como o processamento e a comunicação dos mesmos (Rascão, 2008, p. 73).

APÊNDICE 2 - Mapa Concetual

Pergunta Derivada 1 - *Em que medida a atual capacidade de ciberdefesa nacional será eficaz para fazer face a um ciberataque?*

HIPOTESE	CONCEITOS	DIMENSÕES	INDICADORES
A atual capacidade de ciberdefesa nacional é ineficaz para fazer face a um ciberataque.	*Capacidade de Ciberdefesa Nacional*	Prevenção	EMGFA (CMG Sousa Pereira + CENCOMSTIC / COC) IDN / FCCN / CERT / CSIRT / GNS / ANS CERT (Eng.º Lino Santos) / CIIWA / SCEE Marinha CTen Neves (DITIC) Exército (TCor Viegas Nunes) Força Aérea (Cap António Valente) OTAN Trabalhos IESM
		Deteção	
		Defesa	
		Recuperação	
	Ciberataque	Domínio Governo	MDN / MAI / MNE GNS / ANS Sistema de Certificação Eletrónica do Estado (SCEE)
		Domínio Militar	Marinha / Exército / Força Aérea
		Domínio Civil	REN; Telecomunicações; Transportes; Sistema Financeiro; Distribuição de Água, Serviços de Emergência.

Pergunta Derivada 2 - *De que forma será necessário desenvolver as capacidades de ciberdefesa nacionais para melhorar e complementar as existentes?*

HIPOTESE	CONCEITOS	DIMENSÕES	INDICADORES
As capacidades de ciberdefesa nacionais terão de ser desenvolvidas de forma conjunta, combinada e integrada com as estruturas civis.	*Conjunto*	Marinha Exército Força Aérea MDN MAI MNE	EMGFA (MGen Aires / CFR Sousa Pereira + CENCOMSTIC / COC) Marinha CTen Neves (DITIC) Exército (TCor Viegas Nunes) Força Aérea (TCor Alves / Cap António Valente)
	Combinado	OTAN	NAC; CDMB; NC3; NMA; NCSA; CCDCoE National Cyber Security Policies and Strategies (Frameworks CCDCoE 2011)
		UE	*EU Policy on Network and Information Security* *ENISA - European Network and Information Security Agency*
		EDA	Gérard Lapierre Resultados do *Cyber Defense Project Team*
	Estruturas Civis	REN; Telecomunicações; Transportes; Sistema Financeiro; Distribuição de Água, Serviços de Emergência.	REN; Telecomunicações; Transportes; Sistema Financeiro; Distribuição de Água, Serviços de Emergência.

ANEXO A

Organização do Gabinete Nacional de Segurança

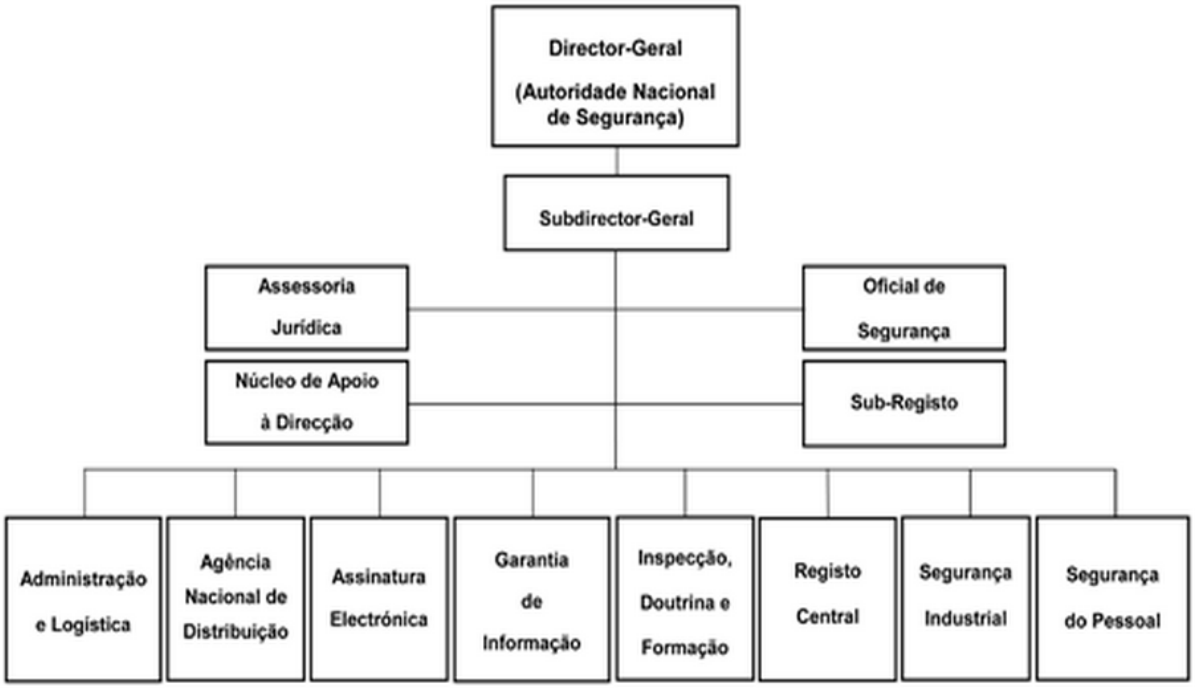

Figura 3 - Organização do GNS.

Fonte: www.gns.gov.pt/gns/pt/organograma.

ANEXO B

Centro de Gestão da Rede Informática do Governo

A promoção das tecnologias de informação e comunicação, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade da informação e do governo eletrónico (*e-Government*), envolvem, para certos fins específicos, mecanismos de autenticação digital forte de identidades e assinaturas eletrónicas. A utilização das denominadas infraestruturas de chaves públicas, como por exemplo as associadas com o cartão do cidadão; o passaporte eletrónico português; a disponibilização de serviços da Administração Pública pela internet que requeiram autenticação digital forte de identidades e assinaturas eletrónicas; e a desmaterialização dos processos intra e interorganismos do Estado que requeiram esse tipo de autenticação (SCEE, 2012).

A análise de infraestruturas de chaves públicas de outros Estados, a avaliação da necessidade de criação de um destes sistemas para o Estado Português, e a proposta de recomendações para a sua constituição, foram objeto de um estudo levado a cabo pela Agência para a Sociedade do Conhecimento, em colaboração com a FCCN, a Autoridade Nacional de Comunicações (ANACOM) e o GNS. Neste sentido, o Governo criou uma ECEE (Figura 4), que garante a satisfação das necessidades da sociedade e do Estado nesta área, designando um grupo de trabalho para acompanhar o processo de instalação (SCEE, 2012).

O CEGER constitui o organismo responsável pela gestão da rede informática do Governo e visa apoiá-lo nos domínios das tecnologias de informação e de comunicações e dos sistemas de informação. Por delegação do Primeiro-Ministro, o CEGER funciona na direta dependência do Secretário de Estado da Presidência do Conselho de Ministros (Decreto-Lei nº 163/2007, de 3 de Maio). O CEGER dirige a ECEE, no âmbito SCEE. O CEGER dirige ainda a Entidade Supervisora das Plataformas Eletrónicas no âmbito do Código dos Contratos Públicos. A Segurança da Informação e a Garantia de Informação são uma das principais áreas estratégicas de atuação do CEGER. (CEGER, 2012).

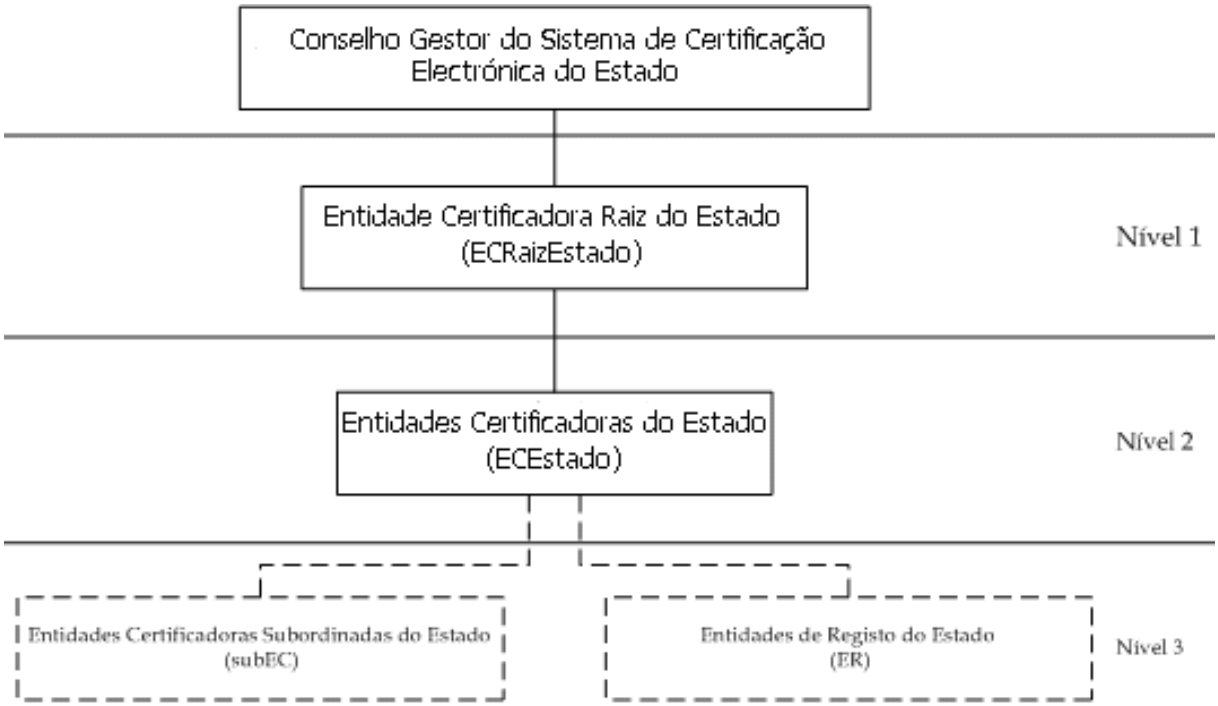

Figura 4 - Estrutura do ECEE.

Fonte: www.scee.gov.pt/ECEE/pt/introducao/org.

Figura 5 - Edifico da Segurança de Informação do CEGER.

Fonte: www.ceger.gov.pt/index.php/pt/seguranca/estrategia.

ANEXO C

International Cyber Incidents (Extrato relativo à Estónia e à Geórgia)

ENEKEN TIKK KADRI KASKA LIIS VIHUL

INTERNATIONAL CYBER INCIDENTS
LEGAL CONSIDERATIONS

CCDCOE
Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia

IV Summary of the Estonian case

INCIDENT TIME FRAME

Start Friday, 27 April 27 2007

End Friday, 18 May 2007 (some aftermath until end of May 2007)

Duration 3 weeks

INCIDENT CONTEXT

Political context and background of incident

- Government decision to relocate a Soviet-era WWII memorial from a central location in the capital city to a military cemetery met by intense opposition from the Russian government and media;
- Protests against the start of removal works break into street riots;
- Siege of the Estonian embassy in Moscow conducted by *Nashi*, a Russian political youth movement. Ambassador physically harassed.

Information society indicators

- Pioneer since mid-1990ies in state-wide public e-solutions employed by both the private and public sectors (prevalent use of Internet banking; mobile parking and public transportation tickets; online voting in elections since 2005; majority or taxes declared electronically; online State Portal as a one-stop service point for all government e-services)
- Internet access nearly universally available (98% of territory), mobile penetration nearing 100% (in 2007);
- Overarching governance policy, backed by a legal framework, to use information technology to increase public sector administrative capacity and ease citizen-to-government communications. Paperless government since 2001.

INCIDENT FACTS

Methods

- DoS and DDoS;
- Website defacement;
- Attacking DNS servers;
- Mass e-mail and comment spam.

Targets

- Servers of institutions responsible for the Estonian Internet infrastructure;
- Governmental and political targets (parliament, president, ministries, state agencies, political parties);
- Services provided by the private sector (e-banking, news organisations);
- Personal and random targets.

Origin

- Mainly sourced outside of Estonia, computers involved from 178 countries altogether;
- Early attacks largely carried out by nationalistically/politically motivated individuals and following instructions provided on Russian-language Internet forums and websites;
- The second phase of attacks has features of central command and control;
- A few self-proclaimed or self-acknowledged attackers;
- Russian authorities have denied any involvement.

Effect

- Perceptible effect to the functioning of domestic economy: affecting sectors of commerce, industry and governance that rely on ICT infrastructure and electronic communications in their daily conduct of business (banks, media corporations, governmental institutions, small and medium size enterprises);
- Societal effect: hindered access to communication with public administration (unavailability of information, means of communication, and access to services);
- Information flow to the outside world im-

paired;

- Side-effects: attack mitigation means blocked off part of the genuine traffic together with the malicious one.

Measures taken

- Response coordinated by CERT-EE, with assistance from system administrators and experts both within and outside of the country; IT experts from both public and private sectors engaged round-the-clock;
- Technical measures: increasing bandwidth, using multiple servers and/or connections; firewalling, filtering out malicious traffic; application of security patches; use of attack detection systems, etc. Some sites temporarily switched to "lightweight mode";
- International cooperation, organised by Ministry of Defence: informing partners in EU and NATO; observer and advisory assistance from NATO network incident handling entities; national CERTs (e.g. U.S.A., Germany, Finland) assisted in locating and reporting sources of attack;
- Public awareness: news about Estonia cooperating with foreign authorities to locate cyber criminals and bring them to justice reduced the number of spontaneous attackers.

LEGAL LESSONS IDENTIFIED AND LEARNED

Core of the case

- Highlighted the need to raise international awareness about crimes against information society;
- Raised the question of efficiency of mutual criminal assistance treaties in a situation where the receiving party is unwilling to cooperate.

Summary

- The traditional view of substantive criminal law considers cyber crime foremost as an economically motivated activity, which may not be sufficient to satisfactorily respond to politically motivated cyber attacks where the damaged legal interest is not the integrity, availability, confidentiality or the proper functioning and use of computer data, programs, or networks, but the political, constitutional, economic or social structure of the state;
- There are often differing legal requirements for what is permissible in criminal proceedings in the countries involved; and the attackers may resort their activities to jurisdictions that the attacked country – or the country receiving a request for assistance – does not recognise, which will foreclose the success of criminal proceedings. International law lacks effective enforcement mechanisms to ensure cooperation from the country in which the attacks originate, if the latter in refuses to cooperate. But international cooperation in criminal matters, in its mainly bilateral nature, may be ineffective even if both parties are willing and able to cooperate, as the Internet facilitates easy splitting up of a given illegal act to several small trails that can be left in a number of countries – such as the formation of a botnet to attack servers in a particular country.

Challenges

- Reorientation from a "whose area of responsibility a particular type of cyber attack might be" to an understanding that a national-scale cyber attack is a problem affecting the society, its security and public order as a whole, and therefore the legal framework needs to specify at what degrees of cyber attacks the different institutions are entitled to and obliged to interfere, and what are the procedural rules and the relevant institutions' terms of reference in case of wide-scale cyber incidents.
- A lack of unison of regulation between countries leads to a fragmented approach toward a phenomenon that knows no borders; a wider platform of multilateral cooperation is therefore needed to handle such threats. Also, the development of international agreements and uniform standards of best practice by the relevant international players would be highly welcome, specifying the organisational framework, terms of reference, and procedural rules applicable in the event of a cyber attack.

IV Summary of the Georgian case

INCIDENT TIME FRAME

Start Friday, 8 August 2008

End Thursday, 28 August 2008

Duration 3 weeks

INCIDENT CONTEXT

Political context and background of incident

- Armed conflict between the Russian Federation and Georgia over South Ossetia.

Information society indicators

- Low Internet penetration (7% of population in 2008), but percentage rapidly growing;
- Low overall dependence on IT-infrastructure;
- Limited options for Internet connectivity via land routes, strong interconnection dependency on Russia.

INCIDENT FACTS

Methods

- DoS and DDoS attacks;
- Distribution of malicious software (MS batch script) together with attack instructions; exploiting SQL vulnerability;
- Defacement;
- Using e-mail addresses for spamming and targeted attacks.

Targets

- Government sites (President, Parliament, ministries; local government of Abkhazia);
- News and media sites, online discussion forums;
- Financial institutions.

Origin

- Organised Russian hacker groups most likely behind the exploit attacks;
- No evident link to the Russian administration or state organisations guiding or directing attacks; the Russian government has denied any involvement in the cyber assaults;
- No conclusive proof of who was behind the DDoS or defacement attacks.

Effect

- Limiting Georgia's options to distribute information regarding the ongoing Georgian-Russian military conflict to the outside world and the Georgian public, especially during the critical early days of the conflict;
- Main communications network operators affected; problems exacerbated by physical disconnections in the communications network infrastructure caused by war activities;
- Side-effects: smaller ISP-s adversely affected by countermeasures applied.

Measures taken

- Attack mitigation coordinated by Georgian academic sector CERT who assumed the role of national CERT during the cyber attacks;
- A state-mandated block on access to Russian websites for the dual purpose of information control and freeing up bandwidth;
- Relocating services to servers or hosts located abroad;
- Assistance from national CERTs of other countries.

LEGAL LESSONS IDENTIFIED AND LEARNED

Core of the case

- Applicability of Law of Armed Conflicts to cyber attacks occurring during conventional armed conflict;
- Measures available in national law to deal with wide-scale cyber attacks.

Summary

- The right of the injured state to use force as a response against another state depends on the level of involvement of the source state. While state *direction* and/or *support* of attacks can be seen as active involvement

and therefore justify a stronger reaction, mere *toleration* (making no effort to suppress or stop the perpetrators) or *inaction* (being unable to effectively deal with the perpetrators) on behalf of the source state as passive forms of involvement do not make the source state a target of lawful military operations. Also, the remedy has to be proportionate to the threat – the smaller the overall harm arising from the attacks, the less there is reason to speak of holding the state responsible for cyber attacks. While the direct effect of the Georgian cyber attacks is difficult to estimate, the low overall dependence of the Georgian population on online services indicates that the effect of cyber attacks was not serious enough to amount to severe economic damage or significant human suffering. Considering this threshold, it is highly problematic to apply Law of Armed Conflict to the Georgian cyber attacks – the objective evidence of the case is too vague to meet the necessary criteria of both state involvement and gravity of effect.

- Effective response to cyber attacks of scale and type like the Georgia incident are quite limited under law. In the long-term perspective, most value is to be derived from developing a legal and organisational structure that supports the development of a resilient infrastructure and service capacity, and provides a lawful basis to collect the data necessary for investigation of any future cyber attacks. Also important is the promotion of effective international cooperation, as there is no way for a country to coordinate defences against attacks originating from other jurisdictions.

Challenges

- New approaches needed to traditional LOAC principles to provide effective legal remedies under this area of law;
- Continued development of national ICT legal frameworks.